"Friending" Electronic Evidence

How to Subpoena, Obtain,

and Present Electronic Evidence at Trial

The Honorable John M. Tran
Fairfax Circuit Court
19th Judicial Circuit
4110 Chain Bridge Road
Fairfax, Virginia 22030
John.Tran@fairfaxcounty.gov

Michael E. Barnsback
LeClair Ryan
2318 Mill Road, Suite 1100
Alexandria, Virginia 22314
(703) 647-5931 Direct
(703) 647-5993 Fax
(703) 307-7196 Mobile
Michael.Barnsback@leclairryan.com

Alfred L. Carr
Assistant Bar Counsel
Virginia State Bar
707 East Main Street, Suite 1500
Richmond, VA 23219-2800
carr@vsb.org

Special thanks to Bret Lee, Esq., Rae Mueller, law clerk to the Honorable David S. Schell, Linh Ly, law clerk to the Honorable John M. Tran, Sara M. Sakagami, Esq., M. Jarrad Wright, Esq., Kristan Burch, Esq., and James M. McCauley, Ethics Counsel.

Table of Contents

Appendix

Virginia State Bar - CLE Disclaimer

This material is presented with the understanding that the publisher and the author do not render any legal, accounting or other professional service. It is intended for educational and informational use by attorneys licensed to practice law in Virginia. Because of the rapidly- changing nature of the law, information contained in this publication may become outdated. As a result, an attorney using this material must always research original sources of authority and update information to ensure accuracy when dealing with a specific clients legal matters. In no event will the author, the reviewers, or the publisher be liable for any direct, indirect or consequential damages resulting from the use of this material. The views expressed herein are not necessarily those of the Virginia State Bar.

THE HONORABLE JOHN M. TRAN

On April 4, 2013, the Virginia General Assembly elected Judge Tran to serve on the Circuit Court of Fairfax County. His term started on July 1, 2013. Judge Tran is the 63rd Circuit Court judge to serve on the Fairfax Circuit Court bench since 1742.

The son of a South Vietnamese diplomat and an immigrant who found refuge in the United States, he spent his entire adult life in the Washington Metropolitan Area and proudly considers himself a Virginian.

Prior to his appointment on the bench, Judge Tran shaped his trial experience as a state and federal prosecutor in Alexandria, Virginia in the late 1980's and eventually joined the highly regarded Old Town Alexandria litigation boutique law firm of DiMuroGinsberg, P.C.

The diversity of his 29-year career as a trial lawyer, starting off as state and then federal prosecutor, was reflective of trial dockets found in state and federal courts throughout the country. Judge Tran has represented businesses and individuals in matters ranging from simple contract disputes to complex commercial and multi-jurisdictional litigation and criminal defense.

Before leaving the practice of law, Judge Tran was an "AV" rated lawyer under Martindale Hubbell, a Virginia Super Lawyer and Best Lawyer in the area of commercial litigation, and inducted into the Class of 2010 Fellow of the Virginia Law Foundation and Class of 2011 Virginia Lawyer's Weekly Leader in the Law.

He has enjoyed his activities in various bar associations including his two term service on the Virginia State Bar Council following his elections in the 18th Judicial Circuit (Alexandria), his 15+ year involvement with the Asian Pacific American Bar Association of Virginia and his participation as a Director on both the Alexandria Bar Association's Law Foundation and most recently the Fairfax Bar Association's Board of Directors. He has received substantial support throughout his career from the various bar associations dedicated to promoting diversity within the legal profession including NAPABA, APABA-DC, APABA- Md, VABA-DC and NCVAA.

Prior to joining the Circuit Court bench, Judge Tran was appointed a substitute judge in 2008 and served on the General District Courts and Juvenile and Domestic Relations District Court throughout Northern Virginia.

Judge Tran is a product of the Arlington County public school system, a 1981 graduate of the George Washington University and a 1984 graduate of the George Washington University Law School.

MICHAEL E. BARNSBACK

Mr. Barnsback counsels and represents Virginia employers in all aspects of employment law. He has frequently lectured on and assisted employers with disability accommodation and leave issues under the ADA and FMLA. He is experienced defending employers in Department of Labor wage/hour audits and FLSA individual and collective action overtime cases. He also has significant background representing employers before the EEOC and state/local administrative agencies. He has over twenty years of courtroom experience litigating employment related cases. His practice also focuses on protecting employers from unfair competition and theft of trade secrets and confidential information, and breaches of fiduciary duties by employees, officers and directors. Mr. Barnsback has worked extensively with federal government contractors and employers in the healthcare and construction fields. He is an editor of the Virginia Employment Law Letter, a monthly newsletter published by M. Lee Smith Publishers, LLC. Mr. Barnsback also lectures frequently on employment law and human resources issues.

ALFRED L. CARR

Mr. Carr received his bachelor's degree in Business Administration and Management from Virginia Commonwealth University, and his Jurist Doctor degree from the Washington College of Law at American University. Mr. Carr was admitted to the Virginia State Bar in 2001.

Mr. Carr currently serves as an Assistant Bar Counsel for the Virginia State Bar in the Disciplinary Section. He is responsible for investigating and prosecuting attorneys in disciplinary proceedings before disciplinary tribunals and courts across the Commonwealth of Virginia.

Previously, Mr. Carr was an Associate with Fredericks & Stephens where he practiced law in the areas of residential real estate matters, conservator, trustee and guardianship matters, family law, and estate administration issues. Prior to joining Fredericks & Stephens, Mr. Carr was an Associate with the law firm of Mitchell I. Mutnick, P.C. where he also practiced in the areas of real estate law, criminal law, and conservator, trustee and guardianship matters. He joined the law firm of Smith and Greene, PLLC, where he concentrated on the general practice of law including domestic relations, criminal law and civil litigation.

Upon graduation from law school, Mr. Carr served as a Judicial Intern to the Hon. Gerald Bruce Lee of the U.S. District Court, Eastern District of Virginia, Alexandria Division. Before and during law school, Mr. Carr was employed as a Regulatory Accountant at Virginia Power (now Dominion Power) and Potomac Electric and Power Company (PEPCO) where he designed computer models to support rate increase filings. He has also been employed as a computer consultant and a systems analyst at various Fortune 500 corporations including MCI/WorldCom, Freddie Mac, GEICO, and as a Statistical Analysis Software ("SAS") expert for the Economic Analysis Division at the Department of Justice in support of anti-trust cases.

Mr. Carr is a member of the Virginia State Bar, the Fairfax Bar Association, the Northern Virginia Black Attorneys Association, the Old Dominion Bar Association and the George Mason American Inn of Court. He is married to Gayl B. Carr and is the proud father of two children. The Carr's reside in Fairfax, Va.

"Friending" Electronic Evidence
How to Subpoena, Obtain, and Present Electronic Evidence at Trial

By The Honorable John M. Tran and Michael Barnsback[1]

Introduction

Electronic evidence differs from conventional paper documents in its volume, location(s), format, indestructability, dimensions and dynamic nature. *See* Rothstein, *Managing Discovery of Electronic Information*: *A Pocket Guide for Judges, 2nd edition* (2012) at www.fjc.gov and *Sedona Principles Addressing Electronic Document Production, Second Edition* (Sedona Conference Working Group Series, June 2007), www.thesedonaconference.org/publications (referred to as *Sedona Principles*, *Second Edition*)

Electronic evidence continues to affect the discovery landscape and is firmly entrenched as discoverable in civil cases. Virginia Civil Benchbook for Judges and Lawyers, § 1.07[5][f] (2013-2014 ed.) (citing Va. Sup. Ct. R. 4:1(a)) and § 1.07[6][b] (citing Va. Sup. Ct. R. 4:9A).

Since discovery is more limited in criminal cases, there are fewer opportunities to contest the collection of electronic evidence; however, constitutional and admissibility issues are vigorously tested in criminal cases. The tensions between accepting emerging technology and traditional concepts of privacy continue to test the responsiveness of the judiciary.

Judge Paul Grimm, the Chief Magistrate Judge of the United States District Court of Maryland, in *Lorraine v. Markel American Insurance Co.*, 241 F.R.D. 534 (2007), provided

[1] Special thanks to Bret Lee, Esq., Rae Mueller, law clerk to the Honorable David S. Schell, Linh Ly, law clerk to the Honorable John M. Tran, Sara M. Sakagami, Esq., M. Jarrad Wright, Esq., Kristan Burch, Esq., and James M. McCauley, Ethics Counsel.

practitioners with an invaluable roadmap into admitting electronic evidence, explaining as follows:

> The admissibility of electronic stored information ("ESI"), as with any other form of documentary evidence, requires the proponent of such evidence to overcome certain evidentiary hurdles that include (1) establishing the relevance of ESI; (2) whether it is authentic; (3) if ESI is being offered for the truth of the matter asserted, is it hearsay and if so, is there an exception under the hearsay rule to admit the evidence; and is it an original or duplicate and does it matter; (4) (a) is the probative value of the evidence substantially outweighed by (i) the danger of unfair prejudice, or (ii) its likelihood of confusing or misleading the trier of fact; or (b) the evidence is needlessly cumulative.

Id. at 538; *see also* Hon. Paul W. Grimm, Michael V. Ziccardi, Alexander W. Major, *Back to the Future: Lorraine v. Markel American Insurance Co., and New Findings on the Admissibility of Electronically Stored Information*, 42 Akron L. Rev. 357 (2009). The decision is required study for those who regularly have to present electronic evidence at trial.

Whether engaged in civil or criminal litigation, state or federal court, the commencement of litigation should trigger a litigation hold letter on one side and a litigation hold notice to the client(s) or material witness on the other, especially whenever electronic evidence is anticipated to be involved in the case. A sample of a litigation hold letter and notice are appended to these materials.

As with all matters relating to discovery, the more specific the notice and the more tailored the notice is to the facts of the case, the better. And ultimately, as with all matters relating to discovery, meeting and conferring with counsel to anticipate and resolve issues relating to the collection and presentation of electronic evidence is preferable to either the obstructive conduct or hyperbolic claims of spoliation that are present in too many cases.

I. OBTAINING ELECTRONIC EVIDENCE AND PRIVACY CONCERNS.

A. How Can You Subpoena Electronic Evidence from Facebook, Twitter, AOL, Google, Hotmail, LinkedIn etc.?

Answer: You cannot if you are looking for content.

Your ability to obtain electronic evidence from service providers is restricted by federal statute. The Electronic Communications Privacy Act (aka the Stored Communications Act), 18 U.S.C. §§ 2071 *et seq.,* controls what can, and more significantly, what cannot be obtained by subpoena from entities providing electronic communications or remote computing services to the public.

1. Electronic Communications Privacy Act

The Electronic Communications Privacy Act ("Privacy Act") prohibits any person or entity that provides "electronic communication service" or "remote computing service" to the public from divulging contents of communications stored, carried or maintained by the service. 18 U.S.C. § 2702(a)(1) and (2). Disclosure in violation of the Privacy Act can expose the record holder to civil liability. *See, e.g., Theofel v. Farey-Jones,* 359 F.3d 1066 (9th Cir. 2004).

The Privacy Act enumerates several exceptions to the rule that service providers may not disclose the contents of stored messages. Among the disclosures authorized are those that are incidental to the provision of the intended service (18 U.S.C. § 2702(b)(1), (4), (5)); incidental to the protection of the rights or property of the service provider (18 U.S.C. § 2702(b)(5)); made with the consent of a party to the communication or, in some cases, the consent of the subscriber (18 U.S.C. § 2702(b)(3)); related to child abuse (18 U.S.C. § 2702(b)(6)); made to public agents or entities under certain conditions (18 U.S.C. § 2702(b)(7), (8)); related to authorized wiretaps (18 U.S.C §§ 2702(b)(2), 2517, 2511(2)(a)(ii)); or made in compliance with certain criminal or

administrative subpoenas issued in compliance with federal procedures (18 U.S.C. §§ 2702(b)(2), 2703)).

Courts addressing the language in the Privacy Act uniformly hold that the prohibition extends to providing the information in response to civil discovery subpoenas. In a case decided by the United States District Court for the Eastern District of Virginia, *In re Subpoena Duces Tecum to AOL*, the court granted a motion to quash a facially valid subpoena issued to AOL seeking the production "any and all documents, including electronically stored information" related to a non-party witnesses' email account. 550 F. Supp. 2d 606, 608 (E.D. Va. 2008). In the underlying suit, it was alleged that the non-party witnesses had stolen thousands of confidential documents from their former employer by transferring the documents to their AOL email account. *Id. n.3.* In quashing the subpoena, the court reviewed the exceptions enumerated in the language of § 2702(b) and held that "the Privacy Act's enumerated exceptions do not authorize disclosure pursuant to a civil discovery subpoena." *Id*. at 611-12.

Although there are no Supreme Court of Virginia decisions or circuit court decisions addressing the application of the Privacy Act to civil subpoenas, the Virginia Worker's Compensation Commission applied the Privacy Act to quash a subpoena issued to Facebook. In the matter of *Shana Lee Hensley*, No. 232-16-19, the Commission held that, "the ECPA (18 U.S.C. § 2702) covers this situation, and thus, the Commission does not have the authority to compel Facebook to provide the information requested in the subpoena *duces tecum*." 2010 WL 1459750, at *1 (Va. Workers' Compensation Commission Apr. 9, 2010). However, the Commission remanded the matter back to the Deputy Commissioner to consider whether the claimant should be compelled to sign a release authorizing Facebook to provide the requested information.

In addressing whether the Privacy Act includes an exception for civil subpoenas, several courts outside of Virginia also have concluded that electronic communications holders may not produce "content" records in response to a civil subpoena and cannot be compelled by court order to do so. *See, e.g., O'Grady v. Superior Court*, 44 Cal. Rptr. 3d 72 (Cal. Ct. App. 2006); *Theofel*, 359 F.3d 1066; *Fed. Trade Comm'n v. Netscape Communic'ns Corp.*, 196 F.R.D. 559, 559, 561 (N.D. Cal. 2000); *Flagg v. City of Detroit*, 252 F.R.D. 346 (E.D. Mich. 2008).

2. Content vs. Non-Content Information

Section 2702 of the Privacy Act prohibits any covered entity from voluntarily disclosing both the customer's actual communications (content information) and the "record[s] or other information pertaining to [the] customer" (non-content information). The Privacy Act provides for different standards of protection for these two basic forms of information and provides less protection for non-content information. It only prohibits covered providers from disclosing such information to government entities unless certain exceptions are met. This creates a window of possibility to obtain non-content information from covered providers.

a. What is content?

"'Contents', when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8). This definition states what contents includes but does not actually define what it is.

Examples of some relevant case law on this topic includes:

- Some courts have tried to supplement this definition by attempting to clarify what is excluded from the definition of content. *Jessup-Morgan v. Am. Online, Inc*., 20 F. Supp. 2d 1105, 1108 (E.D. Mich. 2008).

- Single words and subject lines in electronic messages are "contents" protected by the Privacy Act. *Optiver Australia Pty, Ltd. & Anor. v. Tibra Trading Pty. Ltd. & Ors*., No. C 12-80242 EJD (PSG), 2013 WL 256771 (N.D. Cal. Jan. 23, 2013).

- Facebook postings have been held to be covered by the Privacy Act, as Facebook is a provider of both Electronic Communications Service and Remote Computing Service stored content. *Crispin v. Christian Audigier Inc.*, 717 F. Supp. 2d 965, 983 (C.D. Cal. 2010).

- Dates and times of access to the site may not constitute content. But at least one court has held that this is content protected by the Privacy Act. *See J.T. Shannon Lumber Co. v. Gilco Lumber, Inc*., Civil Action No. 2:07cv119, 2008 U.S. Dist. LEXIS 104966 (N.D. Miss. Aug. 14, 2008).

b. What is non-content information?

Guidance is very sparse since courts have not directly addressed this issue. One leading scholar offers the following thoughts: "In contrast, logs of account usage, mail header information minus the subject line, lists of outgoing email addresses sent from an account, and basic subscriber information all count as non-content information." Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 Nw. U. L. Rev. 607, 612-13 (2002-2003).

One theoretical approach to distinguishing content and non-content is to divide electronic communications into "payload" (content) and "delivery instructions." The body of an email you write, the photo you upload, and the comment you post on a social network are the substance of what you are communicating, and therefore content. On the other hand, the address to which you sent that email, the account to which you uploaded the photo, or the IP address of the computer you use to post that comment may not be considered content. Even though they may convey

important or sensitive information, they do not contain the message that you are actually trying to communicate to someone else, but rather information about the source or destination of that message.

B. What Can You Obtain from Facebook, Twitter, AOL, Google, Hotmail, etc.?

Answer: Very little, except information about the identity of the subscriber.

Although the Privacy Act restricts the disclosure of content, an exception under the Act permits a service provider to "divulge a record or other information pertaining to a subscriber or other customer ... to any person other than a government entity." 18 U.S.C. § 2702(c)(6). Thus, the Privacy Act allows the disclosure of customer information such as the names, addresses, telephone numbers, email addresses and the MAC[2] addresses of the subscriber. *See TCYK, LLC v. Does 1-87*, 13 C 3845, 2013 WL 5567772 (N.D. Ill. Oct. 9, 2013).

In addition, information can be obtained from sources like Facebook or Google when you can obtain "the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service." 18 U.S.C. § 2703(b)(3).

Alternatively, instead of going to the provider, focus on obtaining discovery from individuals or organizations that are not considered electronic communication service providers. The restrictions regarding disclosure of electronically stored information apply only to a person or entity that provides, to the public, either an Electronic Communications Service (ECS) or a Remote Computing Service (RCS). 18 U.S.C. §§ 2702(a)-(b), 2703(a)-(b) (2006). *See also Wesley College v. Pitts*, 974 F. Supp. 375, 389 (D. Del. 1997) ("[A] person who does not provide

[2] A Media Access Control ("MAC") address is a unique identification code assigned to network interfaces for communications. It is a hardware address that identifies a node (device) on a network. In other words, it identifies hardware, such as computers and cell phones attached to a network.

an electronic communication service [or a remote communication service] ... can disclose or use with impunity the contents of an electronic communication unlawfully obtained from electronic storage.").

C. Balancing a Right of Privacy vs. Right of Full Disclosure under Discovery: Identifying Anonymous Users

The United States Supreme Court has long recognized the right to speak anonymously. In its 1960 decision of *Talley v. California*, the Supreme Court struck down a Los Angeles ordinance that made it illegal to distribute anonymous handbills. 362 U.S. 60, 64-65 (1960). Similarly, in *McIntyre v. Ohio Elections Commission*, the Supreme Court struck down an Ohio statute prohibiting the distribution of anonymous campaign literature. 514 U.S. 334 (1995). In ruling, the Court wrote that an author's decision to remain anonymous was "an aspect of the freedom of speech protected by the First Amendment." *Id.* at 336, 342. The Supreme Court has recognized that the right to remain anonymous extends to speech on the internet. *See Reno v. ACLU*, 521 U.S. 844 (1997).

However, there are limitations on First Amendment protections, including the right to speak anonymously. Parties have the right to seek redress and pierce the veil of anonymity when speech is harmful. *See McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995). Courts have struggled in balancing the First Amendment right to remain anonymous against the interests of individuals harmed by anonymous speech to use subpoenas issued to internet service providers to unmask the author. The Virginia General Assembly addressed the issue with the enactment of Virginia Code § 8.01–407.1 which is titled, "Identity of persons communicating anonymously over the Internet."

Section 8.01–407.1 provides a procedure that must be followed when a person files a subpoena seeking information about the identity of an anonymous individual that engaged in

Internet communications that are allegedly tortious or illegal. Virginia Code § 8.01–407.1(A). All subpoenas seeking such identifying information must follow the procedure listed in the statute. The procedure is intended to balance the competing First Amendment right of anonymity against the right to seek redress for harmful speech. In order to obtain such a subpoena, the party seeking the information must file in the circuit court, at least 30 days prior to the date disclosure is sought, a copy of the subpoena and provide the following supporting information:

(1) he has given notice of the subpoena to the anonymous communicator via the Internet service provider;

(2) (a) communications made by the anonymous communicator are or may be tortious or illegal *or* (b) the plaintiff "has a legitimate, good faith basis to contend that such party is the victim of conduct actionable in the jurisdiction where the suit is filed," Code § 8.01–407.1(A)(1)(a);

(3) other "reasonable efforts to identify the anonymous communicator have proven fruitless," Code § 8.01–407.1(A)(1)(b);

(4) the identity of the anonymous communicator is important, is centrally needed to advance the claim, is related to the claim or defense, or is directly relevant to the claim or defense;

(5) no motion challenging the viability of the lawsuit is pending; and

(6) the entity to whom the subpoena is addressed likely has responsive information.

Virginia Code § 8.01–407.1(A)(1)(a)–(e) and (3).

The statute also has a notice provision which provides that:

> Except where the anonymous communicator has consented to disclosure in advance, within five business days after receipt of a subpoena and supporting materials calling for disclosure of identifying information concerning an anonymous communicator, the individual or entity to whom the subpoena is addressed shall (i) send an electronic mail notification to the anonymous communicator reporting that the subpoena has been received if an e-mail address is available and (ii) dispatch one copy thereof, by registered mail or commercial delivery service, return receipt requested, to the anonymous communicator at his last known address, if any is on file with the person to whom the subpoena is addressed.

Virginia Code § 8.01–407.1(A)(3).

After receiving notice, the anonymous communicator, or any interested party, may file a written objection, motion to quash, or motion for protective order "at least seven business days prior to the date on which disclosure is sought under the subpoena." Virginia Code § 8.01–407.1(A)(4). Finally, "the party to whom the subpoena is addressed shall not comply with the subpoena earlier than three business days before the date on which disclosure is due, to allow the anonymous communicator the opportunity to object." Virginia Code § 8.01–407.1(A)(6).

Recently, the Virginia Court of Appeals considered a First Amendment challenge to Virginia Code § 8.01–407.1. In the case of *Yelp, Inc. v. Hadeed Carpet Cleaning*, 62 Va. App. 678, 752 S.E.2d 554 (2014), the Virginia Court of Appeals upheld the constitutionality of Virginia Code § 8.01–407.1. The case involved an appeal by Yelp of a civil contempt order for its failure to comply with a subpoena *duces tecum* issued by Hadeed Carpet Cleaning seeking the identity of anonymous Doe defendants who had posted unfavorable reviews of Hadeed on the Yelp website. Hadeed had sued the Doe defendants for defamation. In issuing the order enforcing the subpoena, the circuit court found that the subpoena satisfied both the First Amendment and the procedures established by Virginia Code § 8.01–407.1. The *Yelp* decision discusses in detail the history of First Amendment protection for anonymous speech, the limits on the protection and the legislative history of Virginia Code § 8.01–407.1. At the conclusion of that discussion, the Court of Appeals ruled that, "we hold that Code § 8.01–407.1 provides the path of analysis that a circuit court must follow when determining whether to enforce a subpoena *duces tecum* seeking the identity of an anonymous communicator." *Yelp*, 62 Va. App. at 701. The Court of Appeals found that Hadeed and the circuit court properly followed Virginia Code § 8.01–407.1 and that the circuit court did not abuse its discretion in enforcing the subpoena. The

procedure set forth in Virginia Code § 8.01–407.1 must be followed by litigants in Virginia seeking subpoenas to unmask the identity of anonymous authors on the internet.

D. LEO 1495 (Misconduct: Requesting Issuance of Unenforceable Subpoena on Out of State Individual.)

Many of the service providers to which we may consider issuing subpoenas for the purpose of unmasking the identity of anonymous authors are foreign corporations outside Virginia.[3] Although the Uniform Foreign Depositions Act, Virginia Code § 8.01–411, may provide a procedure to issue a subpoena *duces tecum* to foreign corporations, counsel may be tempted to avoid the time consuming and expensive process and simply send a Virginia issued subpoena to the service agent of the corporation in another state. In fact, the materials in the appendix provide information from many Internet service providers indicating that they are willing to accept service at addresses outside of Virginia.

Counsel must be careful in cutting corners. LEO 1495 (1992) provides that it is "improper and violative of DR 1-102(A)(4) for a Virginia attorney to request a Virginia court to issue a subpoena duces tecum to obtain documents from an out-of-state individual, knowing that such subpoena is not enforceable, unless the subject of the subpoena has agreed to accept service." Although Internet service providers identify who may be served with a subpoena, unless the notice from the provider indicates that it has agreed to accept service of the out-of-state (Virginia) subpoena, counsel must be careful to follow the proper procedures to obtain a subpoena under the Uniform Foreign Depositions Act.

[3] The *Yelp* decision also contains a helpful discussion on jurisdiction and service requirements on a foreign corporation doing business in Virginia.

II. 18 U.S.C. § 2703 VS. VA. CODE § 19.2-70.3 (B)

Law enforcement's growing reliance on "orders for disclosure" of electronic content (hereinafter "disclosure order") has required courts to pay closer attention to Virginia Code § 19.2-70.3(B) and 18 U.S.C. § 2703(d).

A. Disclosure Order

The Commonwealth may seek via a disclosure order from "the time the order is sought and extending up to and including the date the provider discloses the records" the following information and access to include:

SAMPLE REQUEST

1. Cell site activations related to all transmitted communication requested;

2. Telephone and/or cellular numbers transmitted to and from, including phone calls, SMS, MMS, and any other data transmission, and direct connections, excluding the contents of the SMS, MMS, or other messages, if applicable.

3. Date, time, and duration of all transmitted communications;

4. Signaling information;

5. Subscriber, MIN/ESN, IMSI, MSID and billing/payment information for the specified cellular/wireless telephone, to include any Customer Account Notes associated with the account; [4]

[4] Mobile Identification Number ("MIN") is a unique 24-bit number assigned by the wireless service provider to each phone it sells or includes in service plans. *MIN definition*, PHONE SCOOP, http://www.phonescoop.com/glossary/term.php?gid=66 (last visited April 21, 2013); Electronic Serial Number ("ESN") is a permanent 32-bit number embedded by the manufacturer that uniquely identifies a wireless communication device. *ESN definition*, PHONE SCOOP, http://www.phonescoop.com/glossary/term.php?gid=45 (last visited April 21, 2013); International Mobile Subscriber Identity ("IMSI") is a globally-unique code number that identifies a GSM subscriber to the network. *IMSI definition*, PHONE SCOOP, http://www.phonescoop.com/glossary/term.php?gid=201 (last visited April 21, 2013); Mobile Station ID ("MSID") is a unique identification number assigned to a wireless phone number that is reprogrammed when the user changes service providers; it can also be called a MIN. *MSID*, WIKIPEDIA, https://en.wikipedia.org/wiki/MSID (last visited April 21, 2013).

6. Subscriber, MIN/ESN, IMSI, MSID and billing/payment information for any other cellular/wireless telephones on this account or that may be identified from these records;

7. An engineering map, showing all cell-site tower locations/addresses, sectors, orientations and horizontal beam width;

8. The physical address/location of all cellular towers in the specified market;

9. Wireless Internet usage and IP connection records to include any IP address assigned to this account's device(s), logon dates and times and length of session, the IP address assigned to each session and any known domain names, and any related cell site information;

10. All subscriber information, call detail records, data transmission records, wireless Internet usage, and IP connection records be provided in an electronic format specified by the police;

11. A list of control channels/radio channels and their corresponding cell sites;

12. That the order cover and be applied to any cellular/wireless MIN/ESN or IMSI that the subscribers of the phones covered by the order may change service to, for the duration of this order;

13. That the Provider shall, upon request, alter or amend any feature or aspect of subscriber's service if the feature or aspect of the service restricts the ability of law enforcement from decoding electronic or other impulses pertaining to dialing and signaling information utilized in call processing;

14. That service provider initiate a GPS or geo-location signal to determine the location of the subject's mobile device on the service provider's network or with such other reference points as may reasonably be available and at such intervals and times as requested by law enforcement;

15. Range to Tower (RTT) Reports.

Additionally, the requests often seek "subscriber information, including the names, addresses, credit and billing/payment information of the subscribers, published and non-published, for the telephone numbers **dialing to or being dialed** from the cellular/wireless phone numbers"

B. Underlying Statutory Provisions

1. Virginia Code § 19.2-70.3: Obtaining records concerning electronic communication service or remote computing service

The portion relevant to a disclosure order states:

> A. A provider of electronic communication service or remote computing service, which, for purposes of subdivisions A 2 through A 4, includes a foreign corporation that provides such services, shall disclose a record or other information pertaining to a subscriber to or customer of such service, excluding the contents of electronic communications, to an investigative or law-enforcement officer only pursuant to:
>
> 1. A subpoena issued by a grand jury of a court of this Commonwealth;
>
> 2. A search warrant issued by a magistrate, general district court or a circuit court;
>
> 3. A court order for such disclosure issued as provided in this section; or
>
> 4. The consent of the subscriber or customer to such disclosure.
>
> B. A court shall issue an order for disclosure under this section only if the investigative or law-enforcement officer shows that there is reason to believe the records or other information sought are relevant and material to an ongoing criminal investigation, or the investigation of any missing child as defined in § 52-32, missing senior adult as defined in § 52-34.4, or an incapacitated person as defined in § 64.2-2000 who meets the definition of a missing senior adult except for the age requirement. Upon issuance of an order for disclosure under this section, the order and any written application or statement of facts may be sealed by the court for 90 days for good cause shown upon application of the attorney for the Commonwealth in an ex parte proceeding. The order and any written application or statement of facts may be sealed for additional 90-day periods for good cause shown upon subsequent application of the attorney for the Commonwealth in an ex parte proceeding. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify the order, if the information or records requested are unusually voluminous in nature or compliance with such order would otherwise cause an undue burden on such provider.

This Code section indicates the following standards:

1. The disclosure order is limited to "a record or other information pertaining to a subscriber to or customer of [a provider of an electronic communication service]."

2. The investigative or law-enforcement officer must show that there is reason to believe the records or other information is "relevant and material to an ongoing criminal investigation [or an investigation for a missing child, missing senior adult, or incapacitated person]."

3. If a Commonwealth attorney can show "good cause," the order and any underlying written application can be sealed for up to 90 days with the possibility of subsequent 90 day extensions if "good cause" is shown for such extensions.

2. 18 U.S.C. § 2703: Required disclosure of customer communications or records

The portion relevant to a disclosure order states:

(c) Records concerning electronic communication service or remote computing service.—

(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity—

(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction;

(B) obtains a court order for such disclosure under subsection (d) of this section;

(C) has the consent of the subscriber or customer to such disclosure;

(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or

(E) seeks information under paragraph (2).

(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the—

(A) name;

(B) address;

(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;

(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

(d) Requirements for court order.--A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

This Code section indicates the following standards:[5]

1. The disclosure order is limited to a "record or other information pertaining to a subscriber to or customer of" an electronic communication service.

[5] Note: 18 U.S.C. § 2703(d) expressly allows disclosure orders pursuant to subsection § 2703(b) for the *contents* of electronic communications if sought by the government.

2. The governmental entity must offer "specific and articulable facts showing that there are reasonable grounds to believe" that the records or other information sought are "relevant and material to an ongoing criminal investigation."

3. The "record[s] or other information" are not limited to those examples listed in (c)(2)(A)-(F). *See, e.g. In re Applications of U.S. for Orders Pursuant to Title 18, U.S. Code Section 2703(d)*, 509 F. Supp. 2d 76, 80 (D. Mass. 2007). Furthermore, if records were limited only to those six categories, an administrative subpoena would always suffice and there would be no need for a disclosure order.

4. A court "may" issue a disclosure order if the standards are met.

5. If a state governmental authority seeks records, the court "shall not issue" a disclosure order if prohibited by the law of the state.

C. Comparing Virginia's § 19.2-70.3(B) and the Federal § 2703(d) Disclosure Orders

As a preliminary matter, disclosure orders pursuant to these sections are *not* warrants and are *not* based on a probable cause standard. Instead, these are purely statutory creatures that do not implicate the Fourth Amendment due to the reasoning espoused by *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979) ("a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties"). In the absence of statutory protections, there would be no limits on the government's ability to obtain these records from service providers.

Additionally, there have been *no* cases – published or unpublished – addressing the scope of § 19.2-70.3.[6] In *United States v. Clenney*, 631 F.3d 658, 666-67 (4th Cir. 2011), the court merely noted that phone records obtained by a police officer were governed by both § 19.2-70.3 and 18 U.S.C. § 2703 because the Virginia statute "imposes similar safeguards on customer

[6] Only four cases even reference § 19.2-70.3. *See United States v. Clenney*, 631 F.3d 658, 667 (4th Cir. 2011); *Belmer v. Commonwealth*, 36 Va. App. 448, 454, 553 S.E.2d 123, 126 (2001); *Cohen v. John Does 1-100*, No. 99-5116, 1999 WL 1419239, at *2 (Loudon Cnty. 1999); *Carter Mach. Co., Inc. v. Gonzalez*, No. Civ.A. 97-0332-R, 1998 WL 1281295, at *4 (W.D.Va. Mar. 27, 1998).

records, requiring a grand jury subpoena, search warrant, or court order to obtain them without customer consent."

As with the pen register/trap and trace statutes where the Virginia statute is considered along with its federal counterpart,[7] § 19.2-70.3(B) is best viewed as the Virginia analogue for § 2703(d). While there are differences between the two statutes, the distinctions are minimal for purposes of disclosure orders. Thus, federal case law provides the best guidance on what standards govern disclosure orders.[8]

The only case that address what "relevant and material" means within the context of § 2703(d) is the WikiLeaks case of *In re Application of the United States for an Order Pursuant to 18 U.S.C. § 2703(d),* 830 F. Supp. 2d 114 (E.D.Va. 2011)(O'Grady, J.) There, the government obtained a § 2703(d) order requiring Twitter to turn over thirteen months of non-content records relating to individuals associated with WikiLeaks, and the targets moved to quash the order, because, *inter alia*, the government failed to make the requisite showing of relevance and materiality. *Id.* at 129. Judge O'Grady found that (1) "specific and articulable facts" have been stated under a sealed affidavit*;* (2) since no constitutional rights were infringed, "there is no need for constitutional avoidance or narrowing; and (3) the court was satisfied with the scope of the order because the information could help place into context other facts and materiality is not a substantial objection and (4) the government was not required to draft their order with precision or limit the theory of the investigation. *Id.* at 130.

D. Two Standards: "shows that there is reason" versus "offer specific and articulable facts"

[7] Va. Code § 19.2-70.2 is "analogous to the federal statutes governing these devices, found at 18 U.S.C. §§ 1322-23."

[8] Note, also, that there appear to be no Virginia cases interpreting § 2703.

There is still a disparity in the standards espoused by the statutes. Section 19.2-70.3(B) requires an officer to "show[] that there is reason to believe the records or other information sought are relevant and material to an ongoing criminal investigation," while § 2703(d) requires the governmental entity to "offer specific and articulable facts showing that there are reasonable grounds to believe" that "the records or other information sought, are relevant and material to an ongoing criminal investigation." The federal statute has the higher standard of "specific and articulable facts." This raises the question of which standard controls a Virginia court's actions.

While other sections of the Electronic Communications Privacy Act, such as 18 U.S.C. § 2712, explicitly provide for express preemption, § 2703 does not have a preemption clause. But "'where the state law stands as an obstacle to the accomplishment and execution of the full objectives of Congress'—we can presume that Congress intended preemption to occur." *Antilles Cement Corp. v. Fortuno*, 670 F.3d 310, 323-24 (1st Cir. 2012) (citing *La. Pub Serv. Comm'n v. FCC*, 476 U.S. 355, 368-69 (1986)). In passing ECPA, Congress felt statutory changes "were needed to update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies." *United States v. Suarez*, 906 F.2d 977, 980 (4th Cir. 1990) (providing background on the objectives of Congress in passing ECPA).

Section 2703(d) appears to have been intended to provide a floor, not a ceiling, for privacy protections. The only component of the subsection addressing state law provides that a state court cannot issue an order if a stricter state law applies: "In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State." Congress therefore allowed for stricter state laws that offer enhanced privacy protections. But looser standards – such as under § 19.2-70.3 – are preempted by § 2703(d) because they interfere

the full accomplishment and execution of Congress's goal in increasing privacy protection to these records.

Accordingly, an issuing court should require "specific and articulable facts" in support of any requirement for a disclosure order. As a shorthand, it may be useful for the Court to consider this the electronic communication equivalent of a *Terry* stop. *See* Stephanie Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data that Congress Could Enact*, 27 Berkeley Tech. L.J. 117, 151-52 (2012) (hereinafter "*Can You See Me Now?*").

E. Records Available Through a Disclosure Order

"Record or other information" is not defined in § 19.2-70.3, Va. Code § 19.2-61, which provides definitions for this chapter, or in § 2703. In *In re Applications of U.S. for Orders Pursuant to Title 18, U.S. Code Section 2703(d)*, 509 F. Supp. 2d 76, 80 (D. Mass. 2007), the court reasoned that "a court must look to the meaning of the terms in their ordinary usage. In the relevant context, a record means something stored or archived. The term information is synonymous with data." *Id*.

1. Basic Records Listed in § 2703(c)(2)(A)-(F)

It is evident that, at the least, the six pieces of information listed in § 2703(c)(2)(A)-(F) can be obtained through a disclosure order. The government could always obtain that through a simple administrative subpoena; it is only when it seeks records or other information exceeding those six types of data that a disclosure order is required. In the Request listed above, numbers 2, 3, 5 (excluding "any Customer Account Notes associated with this account") 6, 9 (excluding "any related cell cite information"), 10, 11, and 13 all fall squarely within § 2703(c)(2)(A)-(F).

2. Requested Modification of Subscriber Service

Request number 14, which is where the government seeks to affirmatively modify the target subscriber's service does not appear to fall within any "ordinary usage" of "record or other information." Disclosure orders are intended to do just that – disclose information held by a communications provider. Compelling an affirmative change in a subscriber's service is well outside the scope of any disclosure order, but it has been sought by law enforcement.

3. Records for all Numbers Connecting with the Targeted Subscriber's Number

The paragraph after the enumerated requests essentially asks for § 2703(c)(2)(A)-(F) information for every telephone number that calls the target subscriber or is called by the target subscriber, as well as the same information for every IP address that the target subscriber connects to. This is an incredibly wide dragnet that necessarily implicates records unrelated to the target subscriber. Both § 19.2-70.3(B) and § 2703(d) limit this information to records "pertaining to *a* subscriber to or customer of such service." But the request here clearly goes well beyond the records of that single subscriber. Because both statutes allow a disclosure order to target only one subscriber or customer, separate disclosure orders for each potential contact number, supported by "specific and articulable facts" should be required.

4. Cell Site Data

The real legal quagmire arises from request numbers 1, 4, 7, 8, 12, 14, 15, 16, which are essentially requests designed to obtain location information about where the target subscriber has used the cell phone at issue. This location data is commonly referred to as cell site data. Neither § 19.2-70.3 nor § 2703 mention location data, indicating at first glance that such data would be

outside the scope of a disclosure order.[9] But federal courts have held that location data in the form of cell site data can be obtained through a disclosure order. Even those courts that do not believe such records can be obtained have relied upon a potential Fourth Amendment violation, not because such information falls outside the scope of a "record or other information." *See, e.g.*, *In re Application of U.S. for an Order Pursuant to 18 U.S.C. § 2703(d)*, 2012 WL 3260215 (S.D. Tex. July 30, 2012).

There is substantial federal case law on this issue as it relates to § 2703(d) orders. These cases indicate that prospective cell site data requires a warrant but historical cell site data generally does not. However, caution is warranted because there has, of yet, been limited analysis of the impact of the United States Supreme Court's ruling in *United States v. Jones,* 132 S.Ct. 945 (2012), the GPS tracking case.

A few courts have found that the Fourth Amendment does apply. *In re Application of the United States for an Order Authorizing the Release of Historical Cell site Info.*, 809 F. Supp. 2d 113 (E.D.N.Y. 2011); *Commonwealth v. Augustine,* 4 N.E.3d 846 (Mass. 2014).

5. Technical Details of Cell Site Data

A brief technical overview of cell site data is necessary to understand the potential Fourth Amendment implications and why the federal courts are fractured. *Can You See Me Now?* provides a comprehensive overview that expands upon the cursory technical explanations in various federal court opinions:

> Service providers maintain large numbers of radio base stations (also called "cell sites") spread throughout their geographic coverage areas. These cell sites are generally located on "cell towers" serving geographic areas of varying sizes,

[9] In the 2013 legislative session, the failed Virginia House Bill 1904 would have amended § 19.2-70.3 to explicitly state that "'location data' of a customer of an electronic communication service or a remote computer service may only be retrieved from the provider by warrant or consent of the customer." 2012 Va. HB1904.

> depending upon topography and population concentration. Service providers are deploying higher-capacity network architectures, with the potential to provide more precise information regarding a phone user's location.
>
> As part of their normal function, mobile phones periodically identify themselves to the nearest cell site as they move about the coverage area . . . when a phone moves away from the cell site with which it started a call and nearer to a different cell site, the call is "handed over" from one cell site to another without interruption . . . .
>
> As such, rural areas tend to have fewer cell sites, each with greater service areas, than urban areas, which generally have far more sites that are spaced closer together. Obviously, the proximity of one cell site to another in a geographic area is one factor in the production of more accurate location data.
>
> Wireless service providers retain detailed logs for diagnostic, billing, and other purposes. These logs reveal the calls and Internet connections made and received by wireless subscribers, as well as detailed technical information regarding the cell sites that were used. Such logs generally only reveal which particular cell site a phone was near at the time of the call.
>
> Data from multiple towers can be combined to pinpoint (or "triangulate") a phone's latitude and longitude with a high degree of accuracy (typically under fifty meters). This triangulated cell site data is generally only available prospectively, either due to a 911 call by a subscriber, or because a law enforcement agency has asked a carrier to collect it. Some carriers do routinely track and record triangulated data, and movement toward this practice is a general trend in the industry, although it is not yet the dominant practice, much less the common policy of all companies. As such, law enforcement agencies can also obtain high-accuracy, triangulated historical data when it is available due to a specific company's data collection practices . . . .
>
> As carriers embrace faster 4G mobile data technologies, they will need even more cell sites, further reducing the coverage area around each tower.
>
> As the coverage area around each traditional cell tower shrinks, and consumers increasingly embrace cellphones in their homes and businesses, single cell site data will become far more accurate--in some cases as good as GPS, and in others pinpointing someone's location to an area the size of a few blocks.

27 Berkeley Tech. L.J. at 126-33; *see also United States v. Hardrick*, Criminal Action No. 10-202, 2012 WL 4883666, at *2 (E.D.La. Oct. 15, 2012). While there is a trend towards cell phone carriers keeping logs that provide increasingly accurate location data, it is simply impossible to

know what kind of information a disclosure order will yield. It is possible that any given order could generate data indicating only that the person was within a several square-mile radius of a cell tower. Or, it could be data that is as accurate as a GPS signal.

6. Prospective Cell Site Data

It is clear that the majority of federal courts to have addressed the issue of prospective cell site data – also referred to as real time cell site data – believe that probable cause and a warrant are needed. *See U.S. v. Jones*, 908 F. Supp. 2d 203, 208 n.5 (D.D.C. 2012) (citing a selection of seventeen separate cases and comparing it with five opinions holding probable cause is not needed). Notably, these cited opinions were all decided before the Supreme Court's ruling in *Jones*, which suggests that there is now even more reason to be weary of issuing a disclosure order for prospective cell site data.[10]

One of the few cases to address prospective cell site data after *Jones* is *United States v. Skinner*, 690 F.3d 772 (6th Cir. 2012). In a divided opinion, the majority determined that the Fourth Amendment was not implicated in real-time tracking of a suspect's cell site data and phone GPS; the § 2703(d) order was sufficient for the government to obtain this information. Relying primarily on *United States v Knotts*, 460 U.S. 276 (1983) – the first beeper case – the court determined that the defendant had no reasonable expectation of privacy. In light of the Supreme Court's decision in *Jones*, the court determined that Justice Alito's five-member concurrence[11] did not suggest that the limited three-day tracking of the defendant in this case rose to the level of a search.

[10] For the same reasons, real-time GPS tracking of a subscriber's phone should also require a warrant.

[11] In a separate concurrence, Justice Sotomayor was unequivocal that, although she fully joined Justice Scalia's majority opinion, "I agree with Justice Alito that, at the very least, 'longer term

Skinner is of interest because it is the only appellate case to tackle this issue since *Jones*. Its reasoning, although not necessarily in direct contradiction to *Jones*, does contradict the D.C. Circuit's opinion in *Jones*, known as *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010), *reh'g denied sub nom. United States v. Jones*, 625 F.3d 766 (D.C. Cir. 2010), *aff'd*, 132 S. Ct. 945 (2012). *Maynard* adopted a "mosaic theory" of surveillance, in which the sum of the whole surveillance is greater than any individual act of surveillance. *Id*. at 561-62.

> Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts.

Id. at 562.

Regardless, the majority of cases (both before and after *Jones*) treat prospective cell site data requests as a search because it allows for real-time tracking of an individual. As such, the issuing court should adopt the majority position and require that a warrant based on probable cause – not a disclosure order – be sought before prospective cell site data is given to the government. *See, e.g., In re Application of United States for an Order Authorizing Disclosure of Location Information of a Specified Wireless Telephone*, 849 F. Supp. 2d 526 (D.Md. 2011).

7. Historic Cell Site Data

GPS monitoring in investigations of most offenses impinges on expectations of privacy.'" *Jones*, 132 S.Ct. at 955 (Sotomayor, J. concurring) (citation omitted). Therefore, a five-member majority of the United States Supreme Court has adopted the basic holding of Justice Alito's concurrence.

A request for historic cell site data if spanned over a period of many months may be arguably worse than *Jones* in which the time period of GPS tracking was four weeks. *Jones*, 132 S.Ct. at 948. As a majority of the Supreme Court held in *Jones* via two concurrences, "relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable. But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." *Id.* at 964 (Alito, J. concurring) (internal citation omitted).[12]

Nevertheless, the lower federal courts have generally – but not uniformly agreed – that historic cell site data is not subject to the Fourth Amendment in the way that prospective cell site data is. In *United States v. Graham*, 846 F. Supp. 2d 384, 396 (D.Md. 2012), the court reviewed relevant case law on the issue of historical cell site data:

> It is well established that Section 2703(c)(1)(B) of the Stored Communications Act applies to historical cell site location data. *See, e.g.*, *In re Application of the United States*, 620 F.3d 304, 313 (3d Cir.2010) (holding that historical cell site location information is "obtainable under at § 2703(d) order"); *In re Applications of the United States*, 509 F.Supp.2d 76, 79–80 (D. Mass. 2007) (historical cell site location information "clearly satisfies" the definitional requirements of § 2703(c) and is therefore obtainable pursuant to a court order issued under § 2703(d)). Magistrate Judge Gauvey of this Court has noted that the type of data at issue in this case is the "least invasive" type of cellular location information and is "commonly sought" under § 2703. *In re Application of the United States*, 849 F.Supp.2d 526, 573, No. 10–2188–SKG, 2011 WL 3423370, at *38 (D.Md. August 3, 2011). The Defendants in this case do not challenge the Stored Communications Act's applicability to the cellular location data at issue.

Although the issue was one of first impression in the court, the court determined that "historical cell site location records are records created and kept by third parties that are voluntarily conveyed to those third parties by their customers. As part of the ordinary course of business,

[12] Justice Sotomayor, in her separate concurrence, explicitly joined this portion of Justice Alito's concurrence. *See Jones*, 132 S.Ct. at 955 (Sotomayor, J. concurring).

cellular phone companies collect information that identifies the cellular towers through which a person's calls are routed." *Id*. at 400.

Drawing a clearer distinction between prospective and historic cell site data, the Massachusetts District Court in *In re Applications of U.S. for Orders Pursuant to Title 18, U.S. Code Section 2703(d)*, 509 F. Supp. 2d at 81, was unconcerned with the potential Fourth Amendment implications of cell tower tracking because the "information will not, however, tell the government anything about the subject's location at the present (or for that matter, his or her location at any given time in the future.)" But ultimately, the court cautioned against making any sweeping Fourth Amendment determination absent an aggrieved defendant.[13] *Id*.

In *Hardrick*, 2012 WL 4883666, at *4, the court acknowledged that, in light of *Jones*, historic cell site data could violate the Fourth Amendment, but the good-faith exception ultimately prevented a ruling on the merits. Nevertheless, courts are divided on the issue:

> The Supreme Court has never decided whether the government must obtain a search warrant before obtaining CSLI [cell site location information], and courts only recently have confronted the issue. A majority of cases hold that a search warrant is not required. *See, e.g., In re Application*, 620 F.3d at 306–08; *United States v. Graham*, 846 F.Supp.2d 384, 404 (D.Md. 2012); *In re Application for an Order Authorizing the Release of Historical Cell–Site Information*, No. 11–MC–0113(JO), 2011 WL 679925, at *2 (E.D.N.Y. Feb. 16, 2011); *United States v. Dye*, NO. 1:10CR221, 2011 WL 1595255, at *9 (N.D. Ohio Apr. 27, 2011); *United States v. Velasquez*, No. CR08–0730 WHA, 2010 WL 4286276, at *4–6 (N.D. Cal. Oct. 22, 2010); *United States v. Benford*, No. 2:09 CR 86, 2010 WL 1266507, at *2–3 (N.D. Ind. Mar. 26, 2010); *Suarez–Blanca*, 2008 WL 4200156, at *8; *In re Applications of the U.S. for Orders Pursuant to 18 U.S.C. § 2703(d)*, 509 F.Supp.2d 76, 80–81 (D. Mass. 2007). A minority hold that a search warrant is required. *See, e.g., In re Application*, 809 F.Supp.2d at 126–27; *In re Application of the U.S. for historical Cell Site Data*, 747 F.Supp.2d 827, 844–46 (S.D. Tex. 2010), appeal docketed, No. 11–20884 (5th Cir. Dec. 14, 2011).

Id. at *6.

[13] One of the frustrating aspects about these cases is that they are almost all *ex parte* proceedings brought by an aggrieved government agency that wants to make use of a § 2703(d) order under seal.

In light of the ongoing legal battle over whether the government needs a warrant to obtain historic cell site data, caution is prudent. While a majority of the Supreme Court in *Jones* clearly suggested that long-term tracking of an individual's whereabouts constitutes a search under the Fourth Amendment, the intersection with *Smith v. Maryland* and its progeny indicates that the standards are likely different where a private company has collected the data. Periodic review of federal case law would be wise to determine if a post –*Jones* consensus arises.

F. Sealing of Records

Only Virginia Code § 19.2-70.3(B) provides that the "order and any written application or statement of facts" may be sealed for 90 days for "good cause shown" upon an application of a Commonwealth attorney. A Commonwealth's attorney may also make an indefinite number of subsequent applications to extend the seal for additional increments of 90 days if "good cause" is shown.

G. Remedies for Violations

There is no suppression remedy for a violation of either § 19.2-70.3 or § 2703 unless the Fourth Amendment or another constitutional provision is violated. *See Clenney*, 631 F.3d at 667. Instead, for statutory violations, "suppression is a creature of the statute" and it must be clearly specified as a remedy.[14] *Id*.; *see also Bansal v. Russ*, 513 F. Supp. 2d 264, 282 (E.D. Pa. 2007) (determining that 18 U.S.C. § 2708 is intended to prevent the application of a suppression remedy). The only protections against ongoing violations of § 19.2-70.3(B) and § 2703(d) are the members of the judiciary.

[14] *Cf*. Va. Code § 19.2-65, which provides for statutory suppression when a wire or oral communication is intercepted in violation of Va. Code § 19.2-61 *et seq*.

1. United States v. Jones (Justice Sotomayor's concerns)

New technology allowing for remote surveillance has prompted calls to adapt Fourth Amendment jurisprudence to respond to the potential for abuse posed by the advancement of technology. Those calls are found in Justice Sotomayor's concurring opinion in *United States v. Jones*, involving the government's use of GPS monitoring, as well as Judge Humphrey's concurring decision in *Foltz v. Commonwealth*, 58 Va. App. 107, 706 S.E.2d 914 (2011)(*en banc*), *aff'd on other grounds*, 284 Va. 467, 732 S.E.2d 4 (2012).

The Fourth Amendment recognizes "[t]he right of the people to be secure in their persons, houses, papers and effects" and protects against unreasonable searches or seizures. The Supreme Court has recognized that assessing whether there has been a violation of the amendment is a flexible analysis because "[w]hat is reasonable depends upon all of the circumstances surrounding the search or seizure and the nature of the search or seizure itself." *United States v. Montoya de Hernandez*, 473 U.S. 531, 537 (1985) (citing *New Jersey v. T.L.O.*, 469 U.S. 325, 337-42 (1985)). "Thus, the permissibility of a particular law enforcement practice is judged by balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate governmental interests." *Delaware v. Prouse*, 440 U.S. 648, 654 (1979). "[T]he reasonableness standard usually requires, at a minimum, that the facts upon which an intrusion is based be capable of measurement against 'an objective standard,' whether this be probable cause or a less stringent test." *Id.* "In most criminal cases," the balancing analysis weighs "in favor of the procedures described by the Warrant Clause of the Fourth Amendment." *Skinner v. Ry. Labor Execs. Ass'n*, 489 U.S. 602, 619 (1989).

As the proponents of expanding Fourth Amendment jurisprudence to address the growing technology ask us to recall that nearly 100 years ago, the United States Supreme Court held in

Olmstead v. United States, 277 U.S. 438 (1928), that the Fourth Amendment did not protect private telephone conversations, a decision fundamentally out of step with the then new technology of telephones.

In explaining its ruling, the *Olmstead* court said that the government action of wiretapping a telephone conversation is unlike opening the mail:

> The United States takes no such care of telegraph or telephone messages as of mailed sealed letters. The [Fourth] amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing [through tapping of the telephone lines outside the home] and that only. There was no entry of the houses or offices of the defendants.
>
> By the invention of the telephone 50 years ago, and its application for the purpose of extending communications, one can talk with another at a far distant place.
>
> The language of the [Fourth] amendment cannot be extended and expanded to include telephone wires, reaching to the whole world from the defendant's house or office. The intervening wires are not part of his house or office, any more than are the highways along which they are stretched.

Id. at 464-65. As time passed, however, that view of the Fourth Amendment protections was found to be too limited, and in 1967, nearly 40 years after the Court allowed the government to tap into telephone lines to listen into telephone calls, the United States Supreme Court overruled *Olmstead* in *Katz v. United States,* 389 U.S. 347, 353 (1967), and held that, under the Fourth Amendment, there is a reasonable expectation of privacy in a telephone conversation, even if the conversation is carried out in a public phone booth.

Today, courts traditionally rely upon a two part test to determine whether a defendant has preliminarily asserted a Fourth Amendment violation. The first part of the test is whether the defendant has manifested a subjection expectation of privacy. The second part is whether society is willing to recognize that expectation as reasonable. *Id.*

In 2012, the United States Supreme Court in *United States v. Jones*, , held that placing a GPS device on a car traveling on a public highway is a "classic trespassory search" that violates the Fourth Amendment if it is done without a search warrant. The majority opinion found it unnecessary to address the privacy issues that surrounded the case.

In her concurring opinion in *Jones*, Judge Sotomayor wrote:

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. E.g., *Smith*, 442 U.S., at 742, 99 S.Ct. 2577; *United States v. Miller*, 425 U.S. 435, 443, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976). This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks....I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection. *See Smith*, 442 U.S., at 749, 99 S.Ct. 2577 (Marshall, J., dissenting) ("Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes"); see also *Katz*, 389 U.S., at 351–352, 88 S.Ct. 507 ("[W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected").

132 S. Ct. at 957.

In *Foltz*, the defendant was a registered sex offender who became a suspect in a series of sexual assaults that were similar to the offenses he had committed in the past. *Foltz,* 58 Va. App. at 111, 706 S.E.2d at 916. Investigators placed a GPS device on a work van driven by the defendant upon confirming that the location and timing of recent attacks corresponded to his work schedule. *Id.* at 112, 706 S.E.2d at 916. After confirming through the GPS tracking that defendant was in the vicinity of new attacks, the police placed defendant under visual surveillance and caught him in the act of assaulting another victim. *Id.*, 706 S.E.2d at 917.

Defendant appealed his conviction and raised as one of his grounds a violation of his Fourth Amendment rights.

The case came before the Court of Appeals for *en banc* review, which decided the case on grounds other than the Fourth Amendment, by finding that regardless of whether placing the GPS device on defendant's vehicle violated the Fourth Amendment, evidence from the visual surveillance of defendant could not be excluded as a fruit of the poisonous tree, but instead was "evidence attributed to an independent source" or "evidence where the connection has become so attenuated as to dissipate the taint." *Id.* at 117, 706 S.E.2d at 919 (citing *Warlick v. Commonwealth*, 215 Va. 263, 266, 208 S.E.2d 746, 748 (1974)).

Two concurring opinions in *Foltz* framed today's continuing debate over the balancing of the right of reasonable expectation of privacy against what society will recognize when individuals expose themselves to emerging technology. Prior to the *Jones* case, law enforcement officers held the reasonable belief that a person who operated a motor vehicle on the public highways had no reasonable expectation of privacy in his movements from place to place. *Foltz* was initially decided in 2011, the year before the *Jones* decision.

Judge Beale, joined by Judge Haley, while acknowledging that the legitimate concerns arising from the use of sophisticated technology such as the GPS device, concluded that placing a GPS device on a company owned van and tracking its movements on the public highways did not implicate the Fourth Amendment.

Judge Humphreys, writing a separate concurring opinion, suggested that reviewing a Fourth Amendment claim on the established principles of a reasonable expectation of privacy no longer is adequate to address the dangers posed by the growth of technology. Judge Humphreys noted that analyzing Fourth Amendment issues on privacy grounds alone neglected another

equally important constitutional right and one expressly stated under the Fourth Amendment, and that was our constitutional right to be "secure" in conducting our lives free from government intrusion. More importantly, advancing technology has drastically changed what may be deem reasonable and as Judge Humphreys asked in *Foltz*, if we appear in public and leave our fingerprints on the glasses or forks we abandon in public restaurants, will this give the police the right to swoop down and take DNA samplings from those items?

III. HOW TO OBTAIN ELECTRONIC EVIDENCE

A. Request for Production of Documents

Document requests to a party should be one of the first discovery tools used to obtain electronically stored evidence (ESI). Requests for production of documents shift the burden of production to the other side, and as discussed below, can help solve authentication issues.

However, care must be taken to craft requests that are narrow and easy to understand. Rule 4:1(b)(7) provides that, "[a] party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost." Broad requests for ESI will likely result in a Rule 4:1(b)(7) objection and lead to a motion to compel or motion for protective order. On the other hand, narrow requests typically reduce the burden of production and the chance that a court would sustain the objection.

Further, counsel needs to decide in advance the form of the ESI to be produced and specify that form in the request. Rule 4:9(b)(iii)(B)(2) provides that, "[i]f a request does not specify the form or forms for producing electronically stored information, or if a responding party objects to the requested form or forms of production, a responding party must produce the information as it is ordinarily maintained if it is reasonably usable in such form or forms, or must produce the information in another for or forms in which it is reasonably usable." Unless an

analysis of the metadata of the ESI is desired or necessary, counsel may be best served by specifically requesting that paper copies of the ESI be produced. If however a detailed analysis is necessary, counsel will likely request that the ESI be produced in its native format and not be converted to some other format before production. Giving advance thought to the format of production and specifying that format in the requests can help avoid objections and discovery motions.

In addition to requesting the production of ESI, Rule 4:9 provides a party the opportunity to directly examine computers and electronic storage devices that may contain relevant ESI. Specifically, Rule 4:9(a) permits in pertinent part "the party making the request, or someone acting on his behalf, to inspect, copy, test, or sample . . . electronically stored information . . . ." This is the section of Rule 4:9 permitting the examination and analysis of computers and electronic storage devices by a computer forensics expert on behalf of a party. *See Albertson v. Albertson*, 73 Va. Cir. 94, *98 (Fairfax Cnty. 2007)("Thus under Rule 4:9, the court has the power to require Plaintiff to produce his actual hard drives so Defendant can "inspect and copy" the writings, photographs, or data compilations stored therein").

Naturally, there are great concerns over the scope of an examination of a party's computer or other electronic storage devices. As the court noted in *Albertson*, such an examination "entails a high probability that immensely personal information will be discovered because of the breadth of the information stored" on the computer to be examined. *Id.* at *101. However, issues of scope should not prevent the examination. Orders can be crafted that establish a protocol for the examination that permit the discovery of relevant evidence, while maintaining the privacy of information not reasonably calculated to lead to the discovery of admissible evidence.

1. Implicit Authentication of Documents Produced

Authenticity relates to the source of document and evidence the document came from where the proponent seeking to admit the document claims it came from. Authenticity does not equate to vouching for the accuracy of the information contained in the document.

Rule 2:901 provides that "The requirement of authentication as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the thing is question is what its proponent claims."

Rule 2:903 provides that "The testimony of a subscribing witness is unnecessary to authenticate a writing unless required by the laws of the jurisdiction whose laws govern the validity of the writing"

Setting aside substantive law that requires authentication of documents by specific persons, there is no reason why litigants should not have to accept the authentication of documents they produce in response to a request for the production of documents, except in those rare instances when the producing party has well-grounded concerns the documents are not authentic and may be forgeries.

There are four and as suggested by prominent authors in Virginia evidence, a possible fifth ground for authenticating a document.

Under Rule 4:9(b)(iii) requires "A party who produces documents for inspection either shall produce them as they are kept in the ordinary course of business or shall organize and label them to correspond with the categories in the request."

Therefore, a party who produces documents in response to a request for production of documents, that production implicates three of the five grounds. Charles E. Friend and Kent Sinclair, *The Law of Evidence in Virginia,* § 17-1, at 1166-67, (7th ed. 2012). First, producing a

document responsive to a request is an admission of the genuineness of the document. Second, a party producing a document responsive to a request has provided circumstantial evidence that the document is what it purports to be. Third, a court may take judicial notice of certain facts – such as a party serving requests for admissions on another party and asking the other party to admit the document is authentic.

Under those circumstances, a handful of federal cases have expressly recognized the applicability of implicit authentication by producing a document. *Vulcan Golf, LLC v. Google, Inc.,* 726 F. Supp. 2d 911, 915 (N.D. Ill. 2010); *Seeds v. Lucero,* 177 F. Supp. 2d 1261, 1265 n.1 (N.M. 2010) (citing *In Re Green Air Crash,* 924 F. Supp. 1511, 1514 (S.D. Ind. 1995), *overruled on other grounds, Mimics, Inc. v. Village of Angel Fire,* 277 F. Supp. 2d 1131 (D. N.M. 2003); *Lorraine v. Markel Am. Ins. Co.,* 241 F.R.D. 534, 552-53 (Md. 2007); *Gallegos v. Swift & Co.,* 237 F.R.D. 633, 641 (Colo. 2006).

And at the same time, the contents of a writing may be proved by the admission of a party without producing the original. Rule 2:1007

B. Request for Admissions (Need of trial courts to award fees)

If the authenticity or genuineness of ESI is expected to be an issue, requests for admissions can help solve the problem. Given that the Privacy Act prohibits service providers from producing the content of information stored by the service, a common method of obtaining such evidence it to capture a screen-shot of the publically available information. Admission requests are particularly useful to authenticate such electronic evidence, including Facebook postings, blogs or websites that counsel has identified and captured.

Rule 4:11(a) provides in pertinent part that, "[a] party may serve upon any other party, a written request for the admission, . . . , of the truth of any matters . . . set forth in the request that

relate to statements or opinions of fact or of the application of law to fact, including the genuineness of any documents described in the request." (emphasis added). The Rule requires that copies of the documents be attached to the request unless they have been otherwise furnished or made available. Even if the documents are available or identifiable from another source, the best practice is to attach a paper copy of the specific document to request and label it with an exhibit number. This avoids any confusion as to the document at issue. Further, if you use exhibit numbers to identify the document in the request and use the same exhibit numbers for trial, it is much easier to seek the admission of the exhibit at trial.

The responding party cannot simply give the excuse of "lack of information or knowledge" to avoid responding to the request. In such a circumstance, Rule 4:11(a) requires the party to state, "that he has made reasonable inquiry and that the information known or readily obtainable by him is insufficient to enable him to admit or deny." In other words, a party will be hard pressed to justify using the "lack of information" excuse to avoid answering admissions concerning his own Facebook or website page.

Failure to properly admit the genuineness of a document subject to a request for admission can come at a price. Rule 4:12(c) provides in pertinent part that, "[i]f a party fails to admit the genuineness of any document . . . as requested under Rule 4:11, and if the party requesting the admissions thereafter proves the genuineness of the document . . . , he may apply to the court of an order requiring the other party to pay him the reasonable expenses incurred in making that proof, including reasonable attorney's fees."

C. Depositions

Depositions may also be used as a method to identify and more importantly to authenticate ESI. A party can use the deposition of a party, including a corporate party

representative, to provide sufficient testimony to lay a foundation for the admission of ESI and to authenticate ESI. Rule 4:5(b)(6) permits a party to require a corporate entity to designate one or more representatives to testify on matters that are "designate[d] with reasonable particularity. As with requests for admissions, a party in his Rule 4:5(b)(6) deposition request can identify with "reasonably particularity" the ESI sought to be authenticated during the deposition. The responding corporate party must provide a witness to testify as to "matters known or reasonably available to the organization." In fact, the responding corporate party has an obligation to ensure that the witness designee take steps to investigate the deposition subjects and be prepared to answer questions on the subjects. *See Martin v. Nordic Group of Cos.*, 61 Va. Cir. 13 (Fairfax Cnty. 2003).

Because a Rule 4:5(b)(6) deposition is the deposition of a party, it can be used by the adverse party for any purpose at trial. *See* Rule 4:7(a)(1). This makes the Rule 4:5(b)(6) deposition a powerful tool for addressing in advance of trial concerns over the admission of ESI as trial evidence.

D. Fifth Amendment Concerns

Parties faced with requests for the production of ESI, particularly when in it involves the inspection of computers or electronic storage devices, may be concerned about the production of incriminating evidence protected under the Fifth Amendment. The Fairfax circuit court squarely addressed this issue in *Albertson v. Albertson*, 73 Va. Cir. 94. In rejecting Fifth Amendment protection for documents discovered during the inspection of a computer in a civil matter, the court reasoned that, "an individual's Fifth Amendment protection from self-incrimination is not implicated when private papers, writings, documents, and books are prepared without

compulsion and are later used to incriminate the individual." *Id.* at *99 (citing *Fisher v. United States*, 425 U.S. 391, 400-01, 409-10 (1976)).

E. Cooperation during Discovery

The volume and expense of electronic evidence has highlighted the need for transparency and collaboration during discovery. The traditional expectation of trial judges that lawyers will engage in meaning dialogue and fulfill their obligation of meeting and conferring has given rise to some courts creating suggested protocols addressing the discovery of electronically stored information, *see* http://www.mdd.uscourts.gov/news/news/esiprotocol.pdf.

Although the issues of disclosing and sharing of search terms and predictive coding are relative uncommon, the decisions under those orders that favor transparency and disclosure are consistent with the idea of eliminating litigation by ambush. *See Da Silva Moore v. Publicis Groupe*, 287 F.R.D. 182 (S.D.N.Y. 2012), *adopted by*, 2012 WL 1446534 (S.D.N.Y. Apr. 26, 2012) and *Global Aerospace v. Landow Aviation L.P.*, Consol. Case No. CL 61040, 2012 Va. Cir. LEXIS 50 (Apr. 23, 2012) (approval of predictive coding). *See also Apple Inc. v. Samsung Elecs. Co.*, Case No. 12-cv-0630-LHK, 2013 U.S. Dist. LEXIS 67085 (May 9, 2013) (requiring Google to provide search terms used to collect documents responsive to a subpoena duces tecum).

Litigants embroiled in electronic evidence discovery must sooner rather than later embrace the value of cooperation. *See* Michael Yager, E-Discovery as Quantum Law: Clash of Cultures – What the Future Portends, 19 Rich. J.L. & Tech 10 (2013) (available at http://jolt.richmond.educ/v19i3/article10.pdf).

IV. HOW TO PRESENT ELECTRONIC EVIDENCE AT TRIAL

A. Authenticity

Electronic evidence as with any other documentary evidence have to be shown to be authentic first. As stated above there are several means of authenticating a document which is equally applicable to electronic evidence.

There must be some evidence, through a witness or otherwise, that the electronic evidence was created, acquired, maintained and preserved without alteration. Whereas Virginia's Rule 2:901 standard is broadly stated as any evidence that is "sufficient to support a finding that the thing in question is what is proponent claims," Rule 901 of the Federal Rules of Evidence is more specific and gives examples of what evidence is sufficient, to include in the highlighted portions below under 901(b) as they relate to electronic evidence. The comparable Virginia case law that supports each of the examples is identified next to the examples:

1. Testimony of a Witness with Knowledge (*Blair v. Commonwealth*, 225 Va. 483, 491, 303 S.E.2d 881, 887 (1983);

2. Nonexpert Opinions about Handwriting (*Adams v. Ristine*, 138 Va. 273, 288, 122 S.E. 126, 129 (1924));

3. Comparison by an Expert Witness or the Nonexpert's Opinion about handwriting (*Adams v. Ristine*, 138 Va. 273, 288, 122 S.E. 126, 129 (1924));

4. Distinctive Characteristics and the Like, including the appearance, content, substance, internal patterns or other distinctive characteristics of the item, taken together with all the circumstances (*Whaley v. Commonwealth*, 214 Va. 353, 356-58, 200 S.E.2d 556, 558-59 (1973)(blood-stained shorts); *Bloom v. Commonwealth*, 34 Va. App. 364, 542 S.E.2d 18 (2001)(content of email communications establishing identity)**;**

5. Opinion About a Voice (*Sabo v. Commonwealth*, 38 Va. App. 63, 561 S.E.2d 761 (2002)(audio));

6. Evidence About a Telephone Conversation;

7. Evidence About Public Records (Va. Rule 2:902);

8. Evidence About Ancient Documents or Data Compilation;

9. Evidence About a Process of System. Evidence showing that it produces an accurate result. (*Midkiff v. Commonwealth*, 280 Va. 216, 694 S.E.2d 576 (2010); *Lee v. Commonwealth*, 28 Va. App. 571, 577, 507 S.E.2d 629, 632 (1998); *Ferguson v. Commonwealth*, 212 Va. 745, 187 S.E.2d 189 (1972)**;** and

10. Methods Proved by a Statute or Rule.

    a. Electronic Signatures. Va. Code §§ 2.2-2007, 2.2-4103, 4.1-209.1, 4.1-212.1, 6.2-2000, 6.2-2014, 8.1A-108, 8.7-103, 17.1-258.4, 24.2-424, 38.2-1802 and for criminal cases, § 18.2-186.3.

Specific examples under Rule 901 of the Federal Rules of Evidence include the following:

1. Records of business and financial transactions. *United States v. Meinberg*, 263 F.3d 1177, 1181 (10th Cir. 2001).

2. Phone Records. *United States v. Salgado*, 250 F.3d 438, 453 (6th Cir. 2001).

3. E-mails. *United States v. Siddiqui*, 235 F.3d 1318, 1322 (11th Cir. 2000).

4. Web Pages. *United v. Bansal*, 663 F.3d 634, 667-68 (3rd Cir. 2011).

5. Html. *ACTONet, Ltd. v. Allou Health & Beauty Care*, 219 F.3d 836, 848 (8th Cir. 2000)

6. Chat-room content and text messages. *United v. Lundy;* 676 F.3d 444, 454 (5th Cir. 2012); *United States v. Tank*, 200 F.3d 627, 630-31 (9th Cir. 2000).

In Virginia, the standard of review for the admission of evidence is to present proof by a preponderance of the evidence. "On factual issues relating to the admissibility of evidence, the burden of persuasion is proof by a preponderance of the evidence." *Rabeiro v. Commonwealth*, 10 Va. App. 61, 64-65, 389 S.E.2d 731, 733 (1990).

Virginia evidentiary rulings fall under an abuse of discretion standard on appeal. *Jones v. Commonwealth*, 38 Va. App. 231, 236, 563 S.E.2d 364, 366 (2002): "The admissibility of evidence is within the broad discretion of the trial court, and a ruling will not be disturbed on appeal in the absence of an abuse of discretion." *Blain v. Commonwealth*, 7 Va. App. 10, 16, 371 S.E.2d 838, 842 (1988).

1. Competing Standards for Authenticating Social Media Evidence in other jurisdictions

There is no Virginia state level standard explicitly dealing with social media evidence. Thus, unless and until one is developed by a Virginia court, social media evidence should follow the same evidentiary standards as any other normal writing that would be offered into evidence.

However, other jurisdictions have developed specific approaches to the admission of social media evidence. The two leading methods are the **Maryland Standard vs. Texas Standard.**

The Maryland standard adds additional requirements to property authenticate social media in order to avoid misattributing social media posts, citing concerns with the possibility that other users could be responsible for the content of posts on a person's social media pages. Maryland thusly presupposes a likelihood of fraud or misattribution with any social media posting.

Texas adopts a more traditional evidentiary approach, requiring just enough circumstantial facts so that a jury could reasonably find that the post was authored by the person claimed by the proponent of the evidence.

a. The Maryland Standard

To properly authenticate social media posts, the admitting party shall present evidence that affirmatively establishes authenticity by either

1. Asking the purported creator if she created the profile, and the post;

2. Searching the internet history and hard drive of the purported creator's computer to determine whether that computer was used to originate the social networking profile and posting in question; or

3. Obtaining information directly from the social networking site to establish the appropriate creator and link the posting in question to the person who initiated it.

In *Griffin v. State,* 19 A.3d 415 (Md. 2011), the Maryland Supreme Court held that printouts of MySpace page could not be authenticated just because the page contained a photo and birthdate of the purported creator of the page.

Connecticut follows this strict standard as the Connecticut Court of Appeals has explained that: "the need for authentication arises in this context because an electronic communication, such as a Facebook message, an e-mail or a cell phone text message, could be generated by someone other than the named sender. This is true even with respects to accounts requiring a unique user name and password, given that account holders frequently remain logged in to their accounts while leaving their computers and cell phones unattended . . . Consequently, proving only that a message came from a particular account, without further authenticating evidence, has been held to be inadequate proof of authorship." *State v. Eleck,* 23 A.3d 818, 822 (Conn. App. Ct. 2011).

b. The Texas standard

Texas's admissions standard is less strict than Maryland's and in *Tienda v. State,* 358 S.W.3d 633, 646 (Tex. Crim. App. 2012), the Texas Court of Appeal affirmed the admission of a MySpace page allowing the State to rely on circumstantial evidence of authenticity by producing photos of the defendant, e-mail addresses using the defendant's name and messages referencing

the acts in question. Under the Texas standard, any issue of lack of authorship goes to the weight and not admissibility of the evidence and the proponent of such evidence need only show:

> 1. Whether a jury could reasonably find the proffered evidence authentic.
>
> 2. Authentication depends on the nature of the evidence and the circumstances of the particular case, and could include direct testimony from a witness with personal knowledge, comparison with other authenticated evidence, or … circumstantial evidence.

Delaware has adopted the Texas standard in *Parker v. State*, 85 A.3d 682, 686-87 (Del. 2014), and the Fourth Circuit in *United States v. Cone*, 714 F.3d 197 (4th Cir. 2013) recognized that e-mails while being properly authenticated must still be admitted under a hearsay exception.

Overall, the Texas standard appears to more closely mirror the law in Virginia. "Authentication is merely the process of showing that a document is genuine and that it is what its proponent claims it to be." *Snowden v. Commonwealth*, 62 Va. App. 482, 485, 749 S.E.2d 223, 225 (2013) (quoting *Owens v. Commonwealth*, 10 Va. App. 309, 311, 391 S.E.2d 605, 607 (1990)); *see also Jackson v. Commonwealth*, 13 Va. App. 599, 602, 413 S.E.2d 662, 664 (1992). This can be accomplished by a variety of evidentiary means, including circumstantial evidence. "The amount of evidence sufficient to establish authenticity will vary according to the type of writing, and the circumstances attending its admission, but generally proof of any circumstances which will support a finding that the writing is genuine will suffice." *Williams v. Commonwealth*, 35 Va. App. 545, 556-57, 546 S.E.2d 735, 741 (2001) (quoting *Walters v. Littleton*, 223 Va. 446, 451, 290 S.E.2d 839, 842 (1982)); see also Charles E. Friend & Kent Sinclair, *The Law of Evidence in Virginia* § 17-1, at 1164 (7th ed. 2012). ("[A]uthentication does not set a high barrier to admissibility, and is generally satisfied by any form of proof that supports a finding that it is what it purports to be.").

B. The Best Evidence Rule

In general, the Best Evidence Rule should not bar the admissibility of electronic documents in most of the forms that they would be introduced in, based on the doctrine of duplicate originals.

"Where the contents of a writing are desired to be proved, the writing itself must be produced, or its absence sufficiently accounted for before other evidence of its contents can be admitted." *Randolph v. Commonwealth*, 145 Va. 883, 889, 134 S.E. 544, 546 (1926) (citation omitted).

Important to note is what is not included under the Best Evidence rule: The Best Evidence Rule in Virginia applies only to the admissibility of the contents of writings. It does not apply to images, movies, or other kinds of media that may be posted on electronic sources. *See Brown v. Commonwealth*, 54 Va. App. 107, 116, 676 S.E.2d 326, 330 (2009); *Midkiff v. Commonwealth*, 54 Va. App. 323, 678 S.E.2d 287 (2009), *aff'd*, 280 Va. 216, 694 S.E.2d 576 (2010).

The Best Evidence Rule calls for the production of the original writing, or a duplicate. But, what is an original in the context of electronic evidence?

A writing is admissible despite the Best Evidence requirement, without requiring an exception, if it can be deemed an original, or duplicate original. *See Allocca v. Allocca,* 23 Va. App. 571, 478 S.E.2d 702 (1996). Duplicate originals are quite simply a copy that is an exact reproduction of the original document.

Duplicate originals consist of, among other things, photocopies, by statute. Va. Code § 8.01-391. However, the law has not explicitly addressed other common methods of preparing the evidence for presentation, such as printouts of documents or electronic versions of

documents. However, such alternative methods would likely survive a best evidence objection. *See Tickel v. Commonwealth,* 11 Va. App. 558, 400 S.E.2d 534 (1991) (addressing the admissibility of computer printouts by implication only, and without directly settling the issue). Additionally, at least one statute has approved of the use of electronic versions of documents to fulfill statutory requirements of originals when the documents are presented in circuit court in a form approved for filing under the Rules of the Supreme Court of Virginia. Va. Code § 17.1-258.6.

Other standard evidentiary concerns to be aware of: Rule 403 (Probative value vs. unfair prejudice, confusion or misleading the Jury)

C. Hearsay

Social media statements made by an opposing party may be considered to be an admission of a party opponent. Va. R. Evid. 2:803(0).[15] However, data that is incidental to the communication or evidence, such as the time and date stamp, IP address, and other metadata, may not be available in the absence of a competent witness.

In those circumstances, one of the more commonly used hearsay exceptions that is likely to be relevant is the business records exception, 2:803(6).[16] This exception will likely be required to establish information that is automatically generated with electronic transactions (For

[15] Va. R. Evid. 2:803(0) reads: [The following are not excluded by the hearsay rule, even though the declarant is available as a witness] A statement offered against a party that is (A) the party's own statement, in either an individual or a representative capacity, or (B) a statement of which the party has manifested adoption or belief in its truth, or (C) a statement by a person authorized by the party to make a statement concerning the subject, or (D) a statement by the party's agent or employee, made during the term of the agency or employment, concerning a matter within the scope of such agency or employment, or (E) a statement by a co-conspirator of a party during the course and in furtherance of the conspiracy.

[16] Va. R. Evid. 2:803(6) reads: [The following are not excluded by the hearsay rule, even though the declarant is available as a witness] A memorandum, report, record, or data compilation, in any form, of acts, events, calculations or conditions, made at or near the time by, or from information transmitted by, a person with knowledge in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make and keep the memorandum, report, record, or data compilation, all as shown by the testimony of the custodian or other qualified witness, unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness. The term "business" as used in this paragraph includes business, organization, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit.

example, time and date information generated from a credit card sign-up). *Chau v. Commonwealth*, Record No. 2613-09-4, 2011 WL 291689 (Va. Ct. App. Feb. 1, 2011) (holding that computer generated information regarding a credit card was not hearsay because it was not produced by an individual, and was reliable because it was produced by a reliable process and used in the regular course of business by the credit card company, and thus, was admissible against defendant).

D. Business Records Exception

Do you need a social media/electronic record employee to testify or verify the accuracy of the recording method if you are going to offer social media as a business record?

Yes, it is very likely that you do, for any information that is not otherwise admissible under another exception. The business records exception does require "proof from the original observers or record keepers." *Smith v. Commonwealth*, 280 Va. 178, 183, 694 S.E.2d 578, 580 (2010) (quoting *McDowell v. Commonwealth*, 273 Va. 431, 434, 641 S.E.2d 507, 509 (2007)). *See also Jenkins v. Commonwealth*, Record No. 0362-13-4, 2014 Va. App. Lexis 8 (Va. Ct. App. Jan 14, 2014) (unpublished) (reversing a conviction for a lack of proper authentication of defendant's Paypal and eBay accounts as a business record).

ETHICS

Alfred L. Carr, Assistant Bar Counsel
Virginia State Bar
707 East Main Street, Suite 1500
Richmond, VA 23219-2800

A. Quick Facts About Legal Ethics (http://www.vsb.org/site/regulation/facts-ethics-social-networking) (Author: James M. McCauley, Ethics Counsel for the Virginia State Bar, February 22, 2011)

1. Rules of Professional Conduct to Consider:

   i. RPC 1.1 Competence

   ii. RPC 1.3 Diligence

   iii. RPC 1.6 Confidentiality

   iv. Legal Ethics Opinion ("LEO") 1842

      1. http://www.vacle.org/leos_list-pg113.aspxABA Formal Opinion 10-457 (Complete List Of Legal Ethics Opinions)

2. Pretexting

3. Lawyer Advertising and Marketing

4. Law Firm Policies Regarding Social Media

5. Social Media Tips

B. Digital Age And Social Networking Fosters New Challenges For Litigation Attorneys: But Helpful Guidance Issued By State Bars (Author: James M. McCauley, Ethics Counsel for the Virginia State Bar, March 31, 2014)

1. Duty of Competence

   i. Learn how to securely use iPhones, iPads, Android Devices, laptops, Wireless Wi-Fi networks, Hotspots, etc.

2. Jim McCauley's Guidelines

   i. Guideline No. 1A – Application of Advertising Rules

   ii. Guideline No. 1B – Prohibited Use of "Specialist" on Social Media

iii. Guideline No. 1C – Lawyer Solicitation to View Social Media and a Lawyer's Responsibility to Monitor Social Media Content.

iv. Guideline No. 2.A – Provision of General Information

v. Guideline No. 2.B: Public Solicitation is Prohibited Through "Live" Communications

vi. Guideline No. 3.A – Viewing a Public Portion of a Social Media Website

vii. Guideline No. 3.B – Contacting an Unrepresented Party to View a Restricted Portion of a Social Media Website

viii. Guideline No. 3.C – Viewing A Represented Party's Restricted Social Media Website

ix. Guideline No. 3.D – Lawyer's Use of Agents to Contact a Represented Party

x. Guideline No. 4.A – Removing Existing Social Media Information

xi. Guideline No. 4.B – Adding New Social Media Content

xii. Guideline No. 4.C – False Social Media Statements

xiii. Guideline No. 4.D – A Lawyer's Use of Client-Provided Social Media Information

xiv. Guideline No. 5.A – Lawyers May Conduct Social Media Research

xv. Guideline No. 5.B – A Juror's Social Media Website, Profile, or Posts May Be Viewed As Long As There Is No Communication with the Juror

xvi. Guideline No. 5.C – Deceit Shall Not Be Used to View a Juror's Social Media Profile

xvii. Guideline No. 5.D – Juror Contact During Trial

xviii. Guideline No. 5.E – Juror Misconduct

C. American Bar Association Standing Committee On Ethics And Professional Responsibility – Formal Opinion 10-457 Lawyers Websites (http://www.americanbar.org/content/dam/aba/migrated/2011_build/professional_responsibility/ethics_opinion_10_457.authcheckdam.pdf)

D. American Bar Association Standing Committee On Ethics And Professional Responsibility – Formal Opinion 11-459 Duty To Protect The Confidentiality Of E-mail Communications With One's Client (http://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/11_459_nm_formal_opinion.authcheckdam.pdf)

E. American Bar Association Standing Committee On Ethics And Professional Responsibility – Formal Opinion 11-460 Duty When Lawyer Receives Copies of a Third Party's E-mail Communications with Counsel (http://www.americanbar.org/content/dam/aba/publications/YourABA/11_460.authcheckdam.pdf)

Quick Facts about Legal Ethics and Social Networking

Updated: Feb 22, 2011

By James McCauley

VSB Ethics Counsel

http://www.vsb.org/site/regulation/facts-ethics-social-networking

Virginia State Bar
An agency of the Supreme Court of Virginia

Diligence (RPC 1.3) and Competence (RPC 1.1) require the lawyer to:

- Understand if/how clients are using social networking;
- Advise clients as to their further use of social networking to their best advantage; and
- Use social networking sites as investigative tools (opposing party, witnesses, jurors).

Virginia State Bar
An agency of the Supreme Court of Virginia

Unintended Relationships:

Despite the informality of social networking, the giving of legal advice to others including friends and acquaintances may create unintended client-lawyer relationships. At the very least, it can create confidentiality and conflicts issues. See LEO 1842 (communications with website visitors). *See also ABA Formal Opinion 10-457 (August 5, 2010) (Lawyer Websites)*

- Legal information of general application about a particular subject or issue is not "legal advice" and should not create any lawyer-client issues for the blogging or posting lawyer. Appropriate disclaimers will assure this conclusion.
- However, if a lawyer by online forms, e-mail, chat room, social networking site, etc. elicits specific information about a person's particular legal problem and provides advice to that person, there is a risk that a lawyer-client relationship will have formed. LEO 1842.

Virginia State Bar
An agency of the Supreme Court of Virginia

Confidentiality

- Messages via Twitter or other social networks must be treated with the same degree of reasonable care as messages via e-mail or other traditional communications.
- Discussion about pending legal matters raises problems, and generally should be left to traditional e-mail format.

Virginia State Bar
An agency of the Supreme Court of Virginia

Pretexting

- Pretextually "friending" someone online to garner information useful to a client or harmful to the opposition violates Virginia Rule 8.4(c) prohibition against "dishonesty, fraud, deceit or misrepresentation."
- Even with a friendly pretext, Rules 4.2 and 4.3 apply to communications with persons represented by counsel or with unrepresented persons.

Virginia State Bar
An agency of the Supreme Court of Virginia

Lawyer Advertising and Marketing

- Statements made on social networks about a lawyer's services may be subject to the advertising rules.
- Name and address of responsible lawyer is required. Rule 7.2(e).
- Disclaimers required for specific case results [Rule 7.2(a)(3)] and specialization claims [Rule 7.4(d)].
- Linked In allows you to ask for and receive "recommendations" from clients, colleagues, etc., which should be edited, if necessary, to ensure they comply with all RPCs.

Virginia State Bar
An agency of the Supreme Court of Virginia

Lawyer Advertising and Marketing

- Client recommendations are analogous to client testimonials, so:
  - You can't have your client say things about you that you can't say, Rule 8.4(a).
  - You probably have a duty to monitor your social network sites and blogs for comments and recommendations that may require revision or deletion.
  - For example, the lawyer cannot permit to remain on his LinkedIn page a client recommendation that says the lawyer is the "best personal injury lawyer in town" because it is a comparative statement that cannot be factually substantiated. Rule 7.1(a)(3).
- Invitations from a lawyer to a prospective client into the lawyer's LinkedIn or Facebook page would likely not fall within Rule 7.3, because the client can always decline the invitation; therefore, the invite is not considered in-person communication with prospective clients.

Virginia State Bar
An agency of the Supreme Court of Virginia

Lawyer Advertising and Marketing

- Disclaimer is required for listing “specialty” on LinkedIn. Rule 7.4(d).
- Blogging is considered communication/advertising and is subject to Rule 7.1 – 7.5, as well as all other RPCs, particularly those that govern public statements made in respect to ongoing criminal matters. Rule 3.6.

Virginia State Bar
An agency of the Supreme Court of Virginia

Law Firm Policies Regarding Social Media

- Lawyers in law firms have an ethical duty to supervise subordinate lawyers and non-lawyer staff to ensure that their conduct complies with applicable rules of conduct, including the ethical duty of confidentiality. See Rules 5.1 and 5.3.
- Law firms need to have policies in place regarding employees' use of blogs and social networking websites during and after normal business hours.

Virginia State Bar
An agency of the Supreme Court of Virginia

Social Media Tips

- **Keep personal and professional interests separate. Facebook is better suited for personal, family, and friend connections.**
- **Remember**: "the whole world is watching!"
- **Frequently monitor and update your posts.**
- **Regard social media as a powerful marketing tool.**

Virginia State Bar
An agency of the Supreme Court of Virginia

Social Media Tips

- **Use the built-in privacy capabilities of the social networking sites, and consider limiting the access of users you are connected with.**
- **Remember that what you put out there is permanent!**
- **Remember the RPCs still apply to all social networking!**

Virtual Law Offices, E-Lawyering and the Delivery of Legal Services Over the Internet Pose Challenges for Lawyer Regulators.

James M. McCauley, Ethics Counsel
Ethics Counsel, Virginia State Bar
June 2013

Because technology changes so rapidly the way lawyers practice, it is impossible for lawyer regulators to keep up. Most recently, regulatory bars are scrambling to develop ethical guidance for virtual law practice. Even the ABA Model Rules do not specifically address virtual law firms. However, in August 2012, the ABA House of Delegates adopted rule changes recommended by the Ethics 20/20 Commission to amend the Model Rules to address issues regarding a lawyer's use of technology, including:

- Model Rule 1.1 (revised Comment [8] to confirm that the duty of competence includes "keeping abreast of … the benefits and risks associated with relevant technology").
- Model Rule 1.4 (revised Comment [4] to reflect changes in communication technology).
- Model Rule 1.6 (added new paragraph (c) requiring lawyers to undertake reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or access to, confidential client information and added comment [18] regarding safeguarding confidential client information).
- Model Rule 1.18 (revised the rule and Comment [2] to clarify when electronic communications give rise to a prospective client-lawyer relationship).
- Model Rule 5.3 (revised the title of rule and Comment [2] and adding Comments [3]-[4] to clarify a lawyer's duties when outsourcing legal work to non-lawyer service providers).
- Model Rule 7.1, Comment [3], Model Rule 7.2, Comments [1]-[3], [5] and Model Rule 7.3, Comments [1], [3] (involving revisions that address a lawyer's use of technology for client development).

On March 29, 2013, the Virginia State Bar's Standing Committee on Legal Ethics issued LEO 1872 on virtual law offices (VLOs), concluding that nothing in the Rules of Professional Conduct prohibit lawyers from practicing "virtually." Prior to issuing LEO 1872, the Committee had opined that a lawyer may provide legal services without having any "face-to-face" contact with the client and may maintain a paperless office, storing the client's file in electronic format. Nothing in the Rules of Professional Conduct requires that a lawyer maintain a physical office space to practice law.

Some lawyers define a VLO as a practice in which the lawyer provides legal services exclusively through a website using a secure Internet portal. Other lawyers consider their practice "virtual" if they provide legal services via electronic communications including e-mail and telephone. Still other lawyers combine technology ("E-lawyering") with a "brick and mortar" office to secure the advantages of both worlds.

Lawyers that practice virtually or use Internet technology to deliver legal services need to consider these issues:

Formation of Attorney-Client Relationship and Client Intake

When communicating with potential clients via a secure website portal, or even a traditional website, lawyers should avoid forming unintended attorney-client relationships by using disclaimers on their websites that "posted information is not legal advice" and that communication via the website does not create an attorney-client relationship or a duty of confidentiality. See LEO 1842 (2008) (addressing lawyers' ethical obligations when interacting with potential clients via a web site). Before entering into an engagement agreement, lawyers should obtain sufficient information from the client to screen for conflicts of interest and ensure that the party they are communicating with is the actual client or someone with authority to act on the client's behalf. Lawyers and law firms have been victims of Internet scams in which the fraudster, posing as a prospective client, obtains funds from the lawyer's escrow account using a fraudulent cashier's check. Lawyers should also remember that Rule 1.18 (b) protects as confidential communications by and between a lawyer and a prospective client. A prospective client is a person who discusses with a lawyer the possibility of forming a client-lawyer relationship, even if no such relationship ensues. Rule 1.18(a).

Confidentiality/Competence

Lawyers must take reasonable measures to safeguard confidential client information on the website portal, including investigating and monitoring third-party providers, limiting access to confidential information and obtaining written assurances from the provider concerning data security and the handling of breaches of confidentiality. If a lawyer cannot evaluate the security of the technology used, the lawyer must seek additional information, or consult with someone who possesses the requisite knowledge to ensure compliance with the lawyer's duties of competence and confidentiality.

Competence/Staff Supervision

In addition to protecting confidential information, the lawyer's duty of competence includes implementing data backup systems for the paperless law office. Also, the lawyer must supervise subordinate attorneys and staff who may be working in various physical locations to ensure compliance with the lawyer's professional obligations. See Va. Rules 5.1 and 5.3 and LEO 1850 (2010)(outsourcing legal services will also require supervision on non-lawyers to ensure that they are competent and determine that they have the appropriate training and skills to perform the tasks requested). See also LEO 1735 (1999)(lawyer's ethical duties when using temporary or contract lawyer).

Duty of Communication

Although the duty to keep the client "reasonably informed about significant developments" and "to promptly respond to reasonable requests for information" might be easier or more expedient through electronic communication, the attorney should see that the client is receiving and understanding the information exchanged via the website portal. The virtual lawyer may also need to manage the client's

expectations regarding the lawyer's response time to a client's communications via the Internet. In certain circumstances, phone conferences, video-conferences or in-person meetings would be more appropriate, if not necessary. Examples might include preparing a client or witness for a deposition or hearing or evaluating competency of a client in regard to estate and trust matters.

Duty of Candor in Advertising

To avoid claims of misleading or false statements under Rule 7.1, lawyers should disclose to potential clients the nature and composition of the firm's virtual law office, relevant practice areas and the jurisdictions where its lawyers are licensed to practice. Leased executive office suites or rental space may be denoted in advertising material only if the lawyer actually uses them to conduct practice or deliver legal services. See LEO 1872. If a lawyer is practicing virtually from their home and does not want to disclose her home address, she must use another office address to comply with Rule 7.1(c), if she uses public communications to advertise her professional services.

Avoiding Unauthorized Practice of Law (UPL)

Because a virtual law firm reaches across jurisdictions, lawyers must avoid the unauthorized practice of law when responding to requests from potential clients outside the jurisdictions where the lawyers are admitted to practice. In Virginia, engaging in the unauthorized practice of law is not only a basis for discipline, it is a misdemeanor. What constitutes the practice of law is a fact-specific determination that is the subject of the Virginia Unauthorized Practice Rules, UPL Opinions and case law. Lawyers admitted in Virginia but practicing virtually in another jurisdiction must be cognizant of that other jurisdiction's rules regarding foreign lawyer practice, whether providing services on a "temporary" or "continuous and systematic" basis.

Virginia Rule 5.5 (d)(2) prohibits a foreign lawyer from establishing a "systematic and continuous presence" for the practice of law in Virginia even if the foreign lawyer is not "physically present" in Virginia when delivering legal services. Comment [4] provides that the a lawyer not admitted in Virginia violates Rule 5.5(d)(2)(i) if the foreign lawyer establishes an office or other systematic and continuous presence for the practice of law. Such "non-physical presence" includes the regular interaction with residents of Virginia for the delivery of legal services in Virginia through exchange of information over the Internet or other means. On the other hand, Comment [4] provides that a foreign lawyer may establish an office or other systematic and continuous presence for the practice of law if the foreign lawyer's practice is limited to areas which by state or federal law do not require admission to the Virginia State Bar. Examples given are federal tax practice before the IRS and Tax Court, patent practice before the U. S. Patent Office, or immigration law.

The Ethics 20/20 Commission published an "issues paper" in June 2012 proposing several options to clarify when virtual practice in a jurisdiction is "systematic and continuous," including identifying relevant factors that lawyers and disciplinary authorities should consider and referring the issue to the Standing Committee on Ethics and Professional Responsibility for an ethics opinion. Some of the factors discussed include:

• the nature and volume of communications directed to potential clients in the jurisdiction;

•whether the purpose of the communications is to obtain new clients in the jurisdiction;

• the number of the lawyer's clients in the jurisdiction;

• the proportion of the lawyer's clients in the jurisdiction;

• the frequency of representing clients in the jurisdiction;

• the extent to which the legal services have their predominant effect in the jurisdiction; and

• the extent to which the representation of clients in the jurisdiction arises out of, or is reasonably related to, the lawyer's practice in a jurisdiction in which the lawyer is admitted to practice.

In this paper the Commission observed that technology has made it possible for a virtual law firm to be physically present in one jurisdiction while having a substantial virtual presence in another. The problem is that it is not sufficiently clear when that virtual presence in another jurisdiction is substantial enough to be "continuous and systematic" for purposes of Rule 5.5. Although the Commission received substantial feedback, it ultimately decided to defer the issue as virtual law practice and the pertinent technology continues to develop. Some bar ethics committees are reluctant to issue opinions addressing technology because of how quickly it changes, rendering the opinion obsolete or passé.

Although technology has changed the way that lawyers practice, the ethical concerns that have recently emerged are not that different from the concerns that arise in more traditional practice. Issues regarding confidentiality and supervision of off-site subordinate lawyers and non-lawyer staff have been covered in earlier ethics opinions regarding outsourcing and contract lawyers. The multijurisdictional practice and UPL issues that VLOs raise have been troublesome for regulators for at least two decades in other more traditional contexts involving cross-border practice using regular mail, telephones and court appearances. Similarly, for years, lawyers have been stung by unintended client-lawyer relationships created by careless informal interaction with third parties. Much of the ethical guidance given long ago still applies now. Lawyers need to use common sense, keep abreast of the changes in how law is practiced, stay current in their area or practice, and adhere to the core fiduciary requirements of the client-lawyer relationship: Control (of the professional relationship),Communication, Competence, Confidentiality, Conflicts (avoidance and management).[1]

[1] Professor Susan Martyn, University of Toledo School of Law, describes what she refers to as "the Five Cs"--the five fiduciary duties the lawyer conduct rules and common law impose on lawyers: control, communication, competences, confidentiality and conflicts. Martyn & Fox, *Traversing the Ethical Minefield*, (3rd Ed. 2013) at 66.

DIGITAL AGE AND SOCIAL NETWORKING FOSTERS NEW CHALLENGES FOR LITIGATION ATTORNEYS: BUT HELPFUL GUIDANCE ISSUED BY STATE BARS

James M. McCauley, Ethics Counsel
Virginia State Bar
March 31, 2014

Social media tools like Face Book, LinkedIn and Twitter have proven necessary for lawyers that do trial work and investigations. Lawyers that do trial work now have an ethical duty to become familiar with and use social media in their investigations and trial preparation. Lawyers that ignore these tools and fail to advise their clients regarding usage of social media have likely fallen below an acceptable level of competence. The consequences of not knowing the ethical "dos" and "don'ts" of social media can be catastrophic. For example, trial lawyers should be well aware that their clients' Face Book pages and other social media accounts contain relevant and discoverable evidence that must be preserved and produced pursuant to a lawful discovery request. *Allied Concrete Co. v. Lester*, 285 Va. 295, 302, 736 S.E.2d 699 (2013)(spoliation of evidence charge against plaintiff and plaintiff's counsel; the trial court sanctioned Murray in the amount of $542,000 and Lester in the amount of $180,000 to cover Allied Concrete's attorney's fees and costs in addressing and defending against the misconduct.).

A lawyer may not obstruct or assist a client in obstructing another party's access to relevant evidence in a civil or criminal proceeding. Rule 3.4(a). Further, a lawyer must respond appropriately to lawful discovery requests, and without frivolous objection. Rule 3.4(e). Once a court has entered an order requiring discovery a lawyer may not disregard or advise a client to disregard that order. Rule 3.4(d). When it comes to a point that a trial court has to sanction a lawyer for failing to comply with an order requiring production of discovery, these rules will have likely been violated. In short, egregious non-compliance with discovery should be reported to the bar.

Although the Virginia State Bar has not issued a formal ethics opinion regarding social networking, it has issued two publications which cover the different ethics issues that may arise when lawyers use or fail to use social media in the preparation of their cases: *See* James McCauley, *Blogging and Social Media for Lawyers: Ethical Pitfalls,* 58 VA. LAWYER at 25 (February 2010); *Quick Facts About Legal Ethics and Social Networking*, posted February 22, 2011 at http://www.vsb.org/site/regulation/facts-ethics-social-networking.

The issues that have ethical implications when lawyers consider using social media include:

- Commenting on pending trials or revealing specific case results without a disclaimer.
- Recklessly criticizing judges or other attorneys, or giving that impression.
- Revealing privileged or confidential information.
- Exposing the law firm to claims of defamation or harassment.
- Sending messages that appear to be legal advice, which can create unintended attorney-client relationships.
- Violating ethics rules against solicitation of legal work.
- Practicing law in a jurisdiction where you are not licensed.

- Receiving messages that contain malware or illegal materials.
- Communicating improperly with persons represented by counsel
- Improper pretextual communications with third parties and witnesses
- Failing to use public information contained in social media that may reveal useful information about an opposing party, opposing counsel, witness or juror.

The New York State Bar Association's litigation section on March 18, 2014 issued a detailed set of *Social Media Ethics Guidelines* explaining what is ethically permitted and forbidden for lawyers using social media networks in their practice. Because the New York Rules of Professional Conduct are quite similar to Virginia's, the NYSBA's Litigation Section's *Social Media Ethics Guidelines* are a good place to start in establishing policies and practices with respect to social media.

The report begins by reminding lawyers that their duty of competence requires that the lawyer know, understand and take use of the functionality of social networking. Citing the ABA's 2012 amendment to MR 1.1:

> To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

I have highlighted the "Guidelines," then have added some comments of my own.

Guideline No. 1A—Application of Advertising Rules.

If the lawyer's blog, FB page or other social media is used only for personal purposes, the advertising rules do not apply. If the social media's use is for predominantly marketing and advertising the lawyer's services, its content must comply with the advertising rules.

If a lawyer uses a blog or other social media for personal use, and not to promote or market the lawyer's practice, the bar cannot regulate that form of speech via the advertising rules. The state's attempt to prohibit or restrict non-commercial speech must survive "strict scrutiny" analysis under the First Amendment. *Hunter v. Virginia State Bar*, 285 Va. 485, 510, 744 S.E.2d 611 (2013)(J. Lemons, dissenting).

Guideline No. 1B—Prohibited Use of "Specialist" on Social Media.

Lawyers and law firms shall not advertise areas of practice under headings in social media platforms that include the terms "specialist," unless the lawyer is certified by the appropriate accrediting body in the particular area.

Note that this guideline does not apply to lawyers who advertise to solicit clients in Virginia, because, unlike New York and Florida, Virginia's Rule 7.4 is more relaxed, and does not prohibit lawyers from stating or claiming to be a "specialist" in area of practice if the claim can be factually substantiated. Rule

7.4, cmt. [1]. But lawyers whose practices extend to other states may be subject to another's jurisdiction's more restrictive rule on specialization claims. For example, lawyers who advertise that they are available to provided legal services in Florida may not accept endorsements on LinkedIn for "skills and expertise" in particular areas of law. Fl. Bar Advisory Advertising Op. (Sept. 11, 2013) (prohibiting attorneys from listing practice areas under the "Skills & Expertise" heading in LinkedIn).

Guideline No. 1C-- Lawyer Solicitation to View Social Media and a Lawyer's Responsibility to Monitor Social Media Content.

When inviting others to view a lawyer's social media network, account, or profile, a lawyer must be mindful of the traditional ethical restrictions relating to solicitation and the recommendations of lawyers.

A lawyer is responsible for all content that the lawyer posts on her social media website or profile. A lawyer is not responsible for information that another person, who is not an agent of the lawyer, posts on a lawyer's website, unless the lawyer prompts such person to post the information or otherwise uses such person to circumvent the ethics rules concerning advertising.

Nevertheless, a lawyer has a duty to monitor her social media profile, as well as blogs, for comments and recommendations to ensure compliance with ethics rules. If a person who is not an agent of the lawyer unilaterally posts content to the lawyer's social media website or profile that does not comply with ethics rules, the lawyer must remove such content if such removal is within the lawyer's control and, if not within the lawyer's control, she must ask that person to remove it.

Guideline No. 2.A: Provision of General Information

A lawyer may provide general answers to legal questions asked on social media. A lawyer, however, cannot provide specific legal advice on a social media network because a lawyer's responsive communications may be found to have created an attorney-client relationship and legal advice also may impermissibly disclose information protected by the attorney-client privilege.

Answering general legal questions posted on a blog or other social media site should not be construed as "giving legal advice" nor does it mean that the lawyer is amenable to discussing possible employment merely by responding to a random unsolicited inquiry. See Rule 1.18 (a). However, a lawyer must be cautious when responding to highly particularized legal questions as answering them may create an unintended attorney-client relationship with the inquirer before a conflicts check can be made. The person should be advised to provide her relevant contact information so that the law firm may contact them to set up an appointment or conference.

Guideline No. 2.B: Public Solicitation is Prohibited Through "Live" Communications

Due to the "live" nature of real-time or interactive computer-accessed communications, which includes, among other things, instant messaging and communications transmitted through a chat room, a lawyer may not "solicit" business from the public through such means. If a potential client initiates a specific request seeking to retain a lawyer during real-time social media communications, a lawyer may respond to such request. However, such response must be sent through non-public means and must be kept

confidential, whether the communication is electronic or in some other format. Emails and solicitation on a website are not considered real-time or interactive communications. This guideline does not apply if the recipient is a close friend, relative, former client, or existing client: although ethics rules would otherwise apply to such communications.

Note that this guideline would not be appropriate for Virginia lawyers because the 2013 amendments to the advertising rules did away with the blanket ban on in-person solicitation in personal injury and wrong death cases. See Va. Rule 7.3. In person solicitation is now permissible in any type of matter provided the solicitation does not involve harassment, undue influence, coercion, duress, compulsion, intimidation, threats or unwarranted promises of benefits or if the person has indicated that she does want to be contacted.

Guideline No. 3.A: Viewing a Public Portion of a Social Media Website

A lawyer may view the public portion of a person's social media profile or public posts even if such person is represented by another lawyer. However, the lawyer must be aware that certain social media networks may send an automatic message to the person whose account is being viewed which identifies the person viewing the account as well as other information about such person.

The "automatic message" that is generated and sent to the person whose profile is viewed could be construed as "communication" for purposes of Rule 4.2. Lawyers should keep this in mind when viewing public profiles of represented persons. My view is that the "automatic message" is not a communication relating to the subject of the representation, and further, it is not a communication by the lawyer or lawyer's agent.

Guideline No. 3.B: Contacting an Unrepresented Party to View a Restricted Portion of a Social Media Website

A lawyer may request permission to view the restricted portion of an unrepresented person's social media website or profile. However, the lawyer must use her full name and an accurate profile, and she may not create a different or false profile in order to mask her identity. If the person asks for additional information from the lawyer in response to the request that seeks permission to view her social media profile, the lawyer must accurately provide the information requested by the person or withdraw her request.

It is permissible for a lawyer to join a social media network to obtain information concerning a witness. Any information in that person's public profile is fair game, even if they are represented. But a lawyer may not send a "friend request" to a witness or third party without disclosing her identity, in New York, and in other jurisdictions the lawyer must also disclose her purpose and involvement in the matter under investigation. Another question is which state's rule will apply if the lawyer and the person solicited are in different states?

In New York, there is no "deception" when a lawyer utilizes her "real name and profile" to send a "friend" request to obtain information from an unrepresented person's social media account. New York

Cty. Bar Ass'n Formal Op. 2010-2 (2010). New Hampshire, however, requires that a request to a "friend" must "inform the witness of the lawyer's involvement in the disputed or litigated matter," the disclosure of the "lawyer by name as a lawyer" and the identification of "the client and the matter in litigation." N.H. Bar Ass'n Ethics Advisory Comm., Op. 2012-13/05 (2012). The San Diego bar requires disclosure of the lawyer's "affiliation and the purpose for the request." San Diego County Bar Ass'n Legal Ethics Comm., Op. 2011-2 (2011). The Philadelphia bar association notes that the failure to disclose that the "intent on obtaining information and sharing it with a lawyer for use in a lawsuit to impeach the testimony of the witness" constitutes an impermissible omission of a "highly material fact." Phila. Bar Ass'n Prof'l Guidance Comm., Op. Bar 2009-2 (2009).

Guideline No. 3.C: Viewing A Represented Party's Restricted Social Media Website

A lawyer shall not contact a represented person to seek to review the restricted portion of the person's social media profile unless an express authorization has been furnished by such person.

Guideline No. 3.D: Lawyer's Use of Agents to Contact a Represented Party

As it relates to viewing a person's social media account, a lawyer shall not order or direct an agent to engage in specific conduct, or with knowledge of the specific conduct by such person, ratify it, where such conduct if engaged in by the lawyer would violate any ethics rules.

Guideline No. 4.A: Removing Existing Social Media Information

A lawyer may advise a client as to what content may be maintained or made private on her social media account, as well as to what content may be "taken down" or removed, whether posted by the client or someone else, as long as there is no violation of common law or any statute, rule, or regulation relating to the preservation of information. Unless an appropriate record of the social media information or data is preserved, a party or nonparty may not delete information from a social media profile that is subject to a duty to preserve.

A lawyer needs to be aware that the act of deleting electronically stored information does not mean that such information cannot be recovered through the use of forensic technology. This similarly is the case if a "live" posting is simply made "unlive."

Guideline No. 4.B: Adding New Social Media Content

A lawyer may advise a client with regard to posting new content on a social media website or profile, as long as the proposed content is not known to be false by the lawyer. A lawyer also may not "direct or facilitate the client's publishing of false or misleading information that may be relevant to a claim."

Guideline No. 4.C: False Social Media Statements

A lawyer is prohibited from proffering, supporting, or using false statements if she learns from a client's social media posting that a client's lawsuit involves the assertion of material false factual statement or evidence supports such a conclusion.

Guideline No. 4.D: A Lawyer's Use of Client-Provided Social Media Information

A lawyer may review the contents of the restricted portion of the social media profile of a represented person that was provided to the lawyer by her client, as long as the lawyer did not cause or assist the client to: (i) inappropriately obtain confidential information from the represented person; (ii) invite the represented person to take action without the advice of his or her lawyer; or (iii) otherwise overreach with respect to the represented person.

Guideline No. 5.A: Lawyers May Conduct Social Media Research

A lawyer may research a prospective or sitting juror's public social media website, account, profile, and posts.

Guideline No. 5.B: A Juror's Social Media Website, Profile, or Posts May Be Viewed As Long As There Is No Communication with the Juror

A lawyer may view the social media website, profile, or posts of a prospective juror or sitting juror provided that there is no communication (whether initiated by the lawyer, agent or automatically generated by the social media network) with the juror.

Guideline No. 5.C: Deceit Shall Not Be Used to View a Juror's Social Media Profile

A lawyer may not make misrepresentations or engage in deceit in order to be able to view the social media, account, profile, or posts of a prospective juror or sitting juror, nor may a lawyer direct others to do so.

Guideline No. 5.D: Juror Contact During Trial

After a juror has been sworn and until a trial is completed, a lawyer may view or monitor the social media profile or posts of a juror provided that there is no communication (whether initiated by the lawyer, agent or automatically generated by the social media network) with the juror.

Guideline No. 5.E: Juror Misconduct

In the event a lawyer learns of possible juror misconduct, whether as a result of reviewing a sitting juror's social media profile or posts, or otherwise, she must promptly bring it to the court's attention.

This comports with a lawyer's duty under Va. Rule 3.5(c). Lawyers must be vigilant and acknowledge that, despite the court's instructions otherwise, jurors can and will do their own online research for information and evidence about the case and post comments and status updates during the course of a trial.

NOTICE OF DUTY TO PRESERVE EVIDENCE TO UNREPRESENTED PARTY

Dear Mr. _____:

BACKGROUND

_____ has filed a lawsuit in the United States District Court for the Eastern District of Virginia against _____. The issues in dispute between the parties include, but are not limited to, the following: _____

_____

_____

DEMAND FOR PRESERVATION OF EVIDENCE

_____'s lawsuit will be governed by the Federal Rules of Civil Procedure, which apply to all suits filed in United States federal courts such as the one in the Eastern District of Virginia. Pursuant to the Federal Rules of Civil Procedure, every party to a lawsuit has a duty to preserve all evidence which could be relevant to the suit. This includes the duty to preserve all electronic evidence, such as emails discussing the incident or related to matters at issue in the suit.

This duty to preserve evidence is broad and extends to all documents, regardless of whether the document is stored electronically (such as email) or in hard-copy and regardless of the type of document. For example, reports, spreadsheets, photographs and videotapes are all considered documents that must be preserved. Furthermore, the duty to preserve this documentary evidence extends to all documents in existence as of the time you reasonably anticipated this litigation.

To ensure that all relevant documents are preserved, you should communicate directly with all employees who have possession or control of potentially relevant evidence, including but not limited to personnel who deal with email retention, deletion, and archiving. You should advise each of these employees to preserve any relevant documents in their custody. Furthermore, you should advise all such persons that any regularly scheduled and/or automatic deletion of email or other electronic documents must be discontinued with respect to any relevant data. In addition, any document destruction (such as shredding of documents) must cease with respect to any relevant documents. All relevant documents, both electronic and paper, must be preserved for the duration of this litigation.

If you have any questions about the details of these obligations, please contact me.

Very truly yours,

NOTICE OF DUTY TO PRESERVE EVIDENCE TO REPRESENTED PARTY

Dear Counsel:

My client(s) _____ will be seeking in discovery electronic data in your clients' custody and control that is relevant to this action, including without limitation emails and other information contained on your clients' computer systems and any electronic storage systems. Our client considers this electronic data to be a valuable and irreplaceable source of discoverable information in this matter.

The issues in dispute between the parties include, but are not limited to, the following:

Given that this litigation has been pending for several months and was anticipated even before that time, we are confident that your clients have already taken steps to preserve this data since they have an obligation to preserve relevant evidence. Thus, no procedures should have been implemented to alter any active, deleted or fragmented data. Moreover, no electronic data should have been disposed of or destroyed. We further trust that your clients will continue to preserve such electronic data throughout this litigation.

If you have any questions concerning this notice, please contact me. Thank you.

Very truly yours,

NOTICE OF DUTY TO PRESERVE EVIDENCE TO A REPRESENTED PARTY PRIOR TO THE FILING OF A LAWSUIT

Dear Counsel:

Based upon the issues raised by _____ in the Letter, dated _____ , 2014, _____ provides notice to _____ to preserve all electronically stored information, copies and backup, as defined by Rule 34 of the Federal Rules of Civil Procedure, along with any paper files which _____ maintains relevant to the topics listed in the subsequent paragraph.

To the extent that the parties cannot resolve their disputes short of litigation, _____ shall be seeking in discovery electronic data in _____'s custody and control that relates to _____, including any obligations which _____ has pursuant to _____. Such duty to preserve includes without limitation emails and other information contained on computer systems and any electronic storage systems, along with any paper files and other records maintained by _____. Our client considers the electronic data to be a valuable and irreplaceable source of discoverable information in this matter.

Given that this dispute has been pending for several months and was anticipated even before that time, we are confident that your clients have already taken steps to preserve this data since they have an obligation to preserve relevant evidence. Thus, no procedures should have been implemented to alter any active, deleted or fragmented data. Moreover, no electronic data should have been disposed of or destroyed. We further trust that your clients will continue to preserve such electronic data throughout this litigation.

If you have any questions concerning this notice, please contact me. Thank you.

Very truly yours,

NOTICE TO CLIENT REGARDING LITIGATION HOLD

ACTION REQUIRED

_____ has filed a lawsuit in the United States District Court for the Eastern District of Virginia against _____. The issues in dispute as raised in the attached complaint include, but are not limited to, the following:

_____

_____

OR

Based upon the issues raised by _____ in the Letter, dated _____ , 2014, _____, a copy of which is attached hereto, effective immediately and until further notice, you must NOT destroy, delete or alter any documents, electronically stored information ("ESI") or other materials that are, or could be relevant, to this potential litigation. This means that for the period **beginning January 1, 2006 and continuing until further notice** you must preserve all documents, ESI or other materials that relate to the following matters described below:

1. All documents and materials relating to the relationship and/or transactions between XXXXXXXXXXXXXX with respect to the XXXXXXXXXXX, including, without limitation, documents and materials related to the negotiation of the XXX Agreements, the transactions evidenced by the XXX Agreements, the performance of the parties to the XXX Agreements, any alleged default or non-compliance by either party with the terms of the XXX Agreements, and any efforts made to amend, modify, suspend or otherwise alter the terms and provisions of the XXX Agreements, or to enforce any rights held by either party under the XX Agreements.

2. All documents and materials reflecting payments made by XXX under the XXX Agreements, all documents and materials received or prepared in connection with any non-compliance or alleged non-compliance involving either party to the XXX Agreements, and all communications with XXX regarding the XXX Agreements, the transactions evidenced thereby, or the performance of either party to the XXX Agreements.

3. All documents and materials sent or given by XXX to XXX, received by XXX from XXX, or created, generated, or prepared by XXX relating to the XXX Agreements or the XXX related to the XXX Agreements, including without limitation, documents and materials related to the transactions evidenced by the XXX Agreements, the performance of XXX or XXX under the XXX Agreements, any alleged default or non-compliance with the terms of the XXX Agreements, and any efforts made to amend, modify, suspend or otherwise alter the terms and provisions of the XXX Agreements, or to enforce any rights held by either party under the XXX Agreements.

4. All documents and materials relating to XXX and the Software, including without limitation any enhancements, changes, or modifications to the Software requested by, discussed with, or involving XXX, or any problems or deficiencies in the Software reported by XXX.

5. All documents and materials relating to (i) XXX, (ii) XXX and XXX, (iii) XXX and XXX, or (iv) any transactions or communications relating to XXX.

You should interpret your obligations under this Notice in the broadest sense possible.

You must immediately suspend any procedure that you control that would delete, destroy or alter any documents, ESI or any other materials that may pertain to the above.

You must ensure that anyone who keeps your files (e.g. off-site storage, etc.) is aware of and adheres to these instructions.

After reviewing this Notice, if you have any questions or concerns please contact XXX at the Office of General Counsel.

SCOPE

For purposes of compliance, you should interpret this Notice to encompass as broad a range of documents, ESI and other materials as possible.

The term "**documents**" includes records and other documents potentially relevant to the above matter, regardless of format, storage media or storage location and regardless of whether such belong to or pertain to XXX or XXX. The term "documents" includes any written, recorded, filmed, electronic, or graphic matter, whether in hard or soft copy. Examples of the types of documents would include, without limitation, letters, memoranda, e-mail, notes, minutes, records, case files, computer files or disks, videotapes, audio tapes, graphs, charts, spreadsheets, powerpoint presentations, demo presentations, statements, notebooks, handwritten notes, applications, agreements, books, pamphlets, periodicals, marketing materials, appointment calendars, and work papers.

It also includes voicemail messages (including those delivered through the unified messaging software), text messages, web site content and documents located on the network and the hard drive on individual computers.

Please maintain a copy of each particular document in your possession, whether it is a draft, a final version, or a copy which differs in any way from a draft or final version (due to handwritten notations, receipt stamp, distribution list, etc.).

Please advise XXX of the manner in which any faxes covered by this Notice were received by you, such as paper copy or via RightFax, and how you maintain copies of faxes (e.g, print them out and keep in file or store on the computer).

Each employee should review all possible locations for applicable documents which are covered by this notice, including, but not limited to, their work computer (includes laptops and desktop units), their home computer, CDs, DVDs, disks, thumb drives, any other removable media, PDAs, and cell phones (business and personal).

If you have retained any documents or materials that would be covered by this Notice on a desktop or laptop computer kept at home, CDs, DVDs, disks, thumb drives, any other removable media, PDAs, or cell phones, please immediately advise XXX for further instructions, in addition to pursuing all such responsive documents and materials. In addition, if you have sent any emails which may be covered by this Notice from email accounts other than your work email account, please immediately advise XXX for further instructions.

Your duty to preserve is ongoing. Therefore, you must continue to comply with the directives in this Notice until you receive word from the Office of General Counsel that this Notice is terminated.

Guidelines For Protection Of Documents, ESI Or Other Materials

1. Don't delay: The directives of this Notice are to be implemented immediately.

2. Hard Copy Documents: Identify whether you (or your Division or Department) are the custodian of any potentially relevant hard copy records, ESI or other documents and materials

that may pertain to this Notice. Check your personal files, as well as shared filing areas and offsite storage.

3. Duplicates: Even minor variations in characteristics, like notes, highlighting, different or additional recipients (such as "bcc's"), differences in e-mail strings and "last modified" information, makes one copy not identical to another. When in doubt about whether something is a duplicate, err on the side of preserving all versions or iterations.

4. Ongoing Preservation/Work In Progress: Unless and until otherwise notified in writing, you are required to preserve any and all newly created or received documents, ESI or other materials related to this matter. If you have ESI subject to this Notice that you anticipate needing for business purposes to modify while this Notice is in effect, please contact XXX immediately for assistance.

5. Updates and Additional Obligations: This Notice may be updated, supplemented or otherwise modified as necessary to capture new or revised document preservation or collection demands.

DiMuroGinsberg PC
ATTORNEYS AT LAW

E-Discovery &
Trial Presentation Software

March 13, 2014

E-Discovery Steps

1. Preservation of Electronically Stored Data (ESI)
2. Collection of ESI
3. Processing Data
4. Reviewing Data
5. Production of Data

(And Reviewing What You Get From the Other Side)

Preservation Of ESI

Preservation Is A Critical But Often Overlooked Component of ESI

- Spoliation – the destruction (or material alteration) of evidence or the failure to preserve property for another's use as evidence
  - Courts Have Broad Authority To Impose Sanctions For Failing to Preserve ESI
    - Sanctions Payments
    - Adverse Inference Jury Instructions
    - Attorneys' Fees & Costs
    - Entry of Default or Dismissal in Most Egregious Cases
- When Do You Have To Preserve ESI?
  - Litigation is actually pending
  - Litigation is reasonably foreseeable

Preservation Of ESI

- Litigation Hold Notice
  - Issued When Litigation Becomes Reasonably Likely
  - Should Periodically Reissue Hold Notice
  - Lawyers Typically Draft Litigation Holds, But Usually Distributed By Management
    - It Is Still Important To Make Sure the “Key Players” Get Notice And To Question Management Distribution Method
    - Send Litigation Hold To Third Parties That Are Within Client’s Control (i.e., vendors, accountants, email providers)
    - Make Sure Client/Employees Know That Relevant Documents Could Be Anywhere
  - **Best Practice**: Help Clients Develop Litigation Hold Policies Before Litigation Begins (i.e., how long to retain documents?)

Preservation Of ESI

- Find Out About Client's Document Retention & Destruction Policies
  - It Is Critical To Stop Any Automated Process That Could Destroy Relevant ESI (i.e., automatic email purges, deleting email accounts of former employees)
- To Avoid Arguments That Documents Were Not Preserved Collect Document Sources Ahead Of Litigation
  - Image Computer Hard Drives Once Litigation Is Anticipated
    - This Is Critical To Avoid Changing Metadata
- Send a Hold Request To The Other Side

Collection, Where Are the Documents?

- Who Are The Right Custodians?
  - Identifying Custodians And Processing Once Will Save A Lot Of Money
  - Often Parties Identify Custodians In Discovery Conferences & Joint Discovery Plans
- Where Are The Documents Located?
  - Here Are Some Of The Places The Client May Store Documents:
    - Computer Hard Drive
    - Personal Hard Drive
    - External Hard Drive
    - Backup Tapes
    - External Media (i.e., CDs, DVDs, Thumb Drives)
    - Smartphones/iPads/Tablets
    - Instant Messaging/Bloomberg Terminal Services
    - Voicemail Systems
    - Networked Computers/Networked Attached Storage
    - Internal Servers
    - Internal Databases

Collection… More Document Sources

- Responsive Documents Are Increasingly In The “Cloud”
  - Third Party Email Providers
    - Free Email: Gmail, Yahoo Mail, Microsoft Outlook Online and Paid Servers
  - Document Management Systems
    - Goggle Docs, Office Web Apps, iCloud, Microsoft SharePoint Servers, Amazon S3, Internet Service Providers,
  - Web Hosting Systems
  - Online Storage Systems
    - Amazon S3, Dropbox, Google Drive, Microsoft OneDrive/SkyDrive, Box (F/K/A Box.net), Sugersync
  - Online Backup Systems
    - Carbonite, Mozy, Amazon, Internet Service Providers
- Social Media
  - Webpages, Chat Rooms, Facebook, Google Plus+, Twitter, YouTube, LinkedIn, Four Square, Tumblr, Flickr, Vine, Instagram, Blogs, Instant Messaging, Pinterest, Skype, MySpace, etc.

Collection Issues To Consider

- Consider Which Custodians, Metadata & Search Fields You Need to Produce
- What Format Are The Documents?
- What Date Ranges Do You Need?
- Can You Maintain Metadata During Collection?
  - How Do You Collect Data Without Changing It?
    - For Example, It Is Really Easy To Change The Time Zone Of A Document
    - Imaging Computers
- What Is The Client's IT Infrastructure?
  - What Do Their Systems Look Like?
    What Programs Do They Run And Use?
  - Do They Have An IT Department That Can Collect?
    - Are They Sophisticated?
    - Do They Know Where All Their Information Is Stored?
    - Interviews Of People On the Ground Are Often Required
- Who Should Be Responsible For The Collection?
  - The Client, A Professional, Or DG?
  - Balancing Costs Against Data Integrity
- Is A Forensic Examination Of A Laptop/Computer System Required
  - Parties Typically Can Produce In Normal Course Unless Spoliation Involved

Processing The Data

- Processing Involves Compiling Data Sources Into Manageable Database
- Searchable/OCR Tiff'ed Images Are Created For Each Page
- Deduplication Is Necessary
  - Declining Costs Of Storage Means Data Explosion
  - Computer Programs Scan Images To Eliminate Duplicates
  - But There Are Different Types Of Deduplication
    - Exact Deduplication v. Non-exact Deduplication
    - Deduplication Across Entire Database v. Limited Deduplication Against Custodians
  - Should Discuss Deduplication At Discovery Conference & With Vendor
- Consider Which Custodians, Metadata & Search Fields You Need to Produce To Make Sure That Data Is Processed

Search Terms

- Search Terms – Search Terms Are Often Negotiated In Advance With Opposing Counsel
  - Need To Understand Syntax Used By Review Tool
  - Make Sure Search Terms Are Not Too Broad (i.e., A Search For Privilege Will Get Every Email From A Law Firm With A Privilege Footer)
  - Use Connectors To Narrow Search
    - Murder /p “John Doe”
  - Use Expanders To Capture Everything
  - Some Searches May Only Apply To Some Custodians
  - Run Test Search

Reviewing Data

- Which Discovery Tool Will Be Used?
  - Government Uses Concordance – Hard To Use, But All Programs Will Provide Concordance Load Files
  - Relativity Is Probably The Most Popular Tool Today
  - Other Choices Include: Kroll Ontrack, Ringtail, Summantion
  - Does It Have Analytics To Track Reviewers Progress
- Review Team
  - In House Or Contract Document Reviewers
    - Size Of Project *v.* Getting People Up To Speed *v.* Costs
  - Train Reviewers On Review Tool And Case Considerations
- Coding Considerations:
  - What Issue Tags Do You Need
    - Privilege, Responsive, Non-Responsive, Hot, Specific Issues
    - Will Depend On Circumstances of Case
  - Document Families? Are They Going To Be Coded Consistently
- Make Sure Reviewers Look for Hidden Text/Cells In Docs
  - Reviewers May Have To Look At Native Files At Times
- How Are You Going To Quality Control Work?
  - A Second/Third Level Review?
  - Have DG Attorneys Do Review For Key Personnel Like CEOs?
  - Spot Checks And/Or Random Sample Reviews?

Reviewing Data

- Privilege Log Considerations
  - Are Reviewers Going To Input Narratives Into Database To Help Generate Log
  - What Other Fields Need To Be In Privilege Log?
- Mass Coding
  - Can You Eliminate Certain Categories Of Documents?
- Understand How Database Works
  - Does Changing Coding On One Document Change Database?
- Redacting Documents
- Technical Problem Documents
- Foreign Language Documents
  - Who Is Going To Pay For Translations?
  - Can You Use A Free Translation Tool?
  - How To Treat Foreign Language Documents Should Be Decided During Discovery Conference

Production

- What Format?
  - Native Files?
    - Common For Excel Spreadsheets
    - Sometimes Parties Demand Native For Other Cases
  - PDF
  - Single Page, OCR'ed Tiffed Images With Load Files
    - Most Common
- What Data Fields Are You Going To Produce?
  - To/From, Custodian, CC, BCC, Subject Line, Date Created
    - Typically Decided In Discovery Protocol
- How Much Lead Time Does Vendor Need?
- Cross Broader Collection/Production Issues
  - European Union Privacy Regulations and Similar Privacy Laws
  - Domestic And Foreign Import/Export Restrictions Such As The International Traffic and Arms Regulations ("ITAR")

Future Trends

- Predictive Coding
- Pre-Collection Analytics
- “Big Data”
- Proposed Changes to the FRCP

E-Discovery Vendors

Develop a Preferred Vendor List

- D4
- FTI Consulting
- Logik
- Merrill
- Stroz Friedberg
- TransPerfect
- UHY (Relativity)

Trial Presentation Software

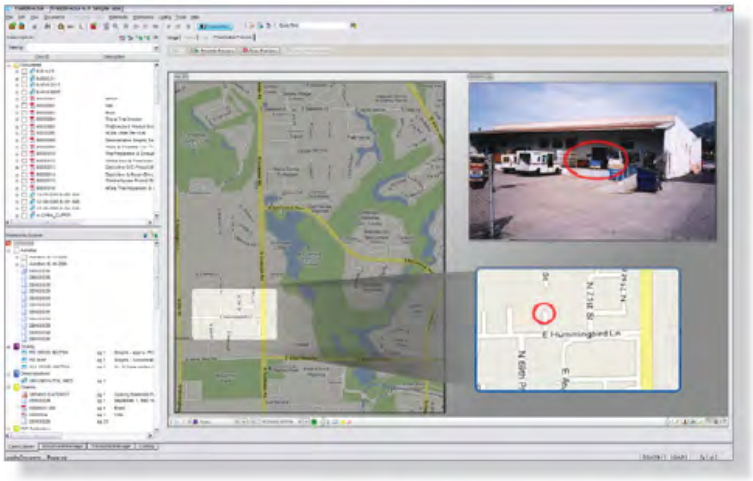
- Display Demonstratives, Exhibits, Deposition Transcripts, Videos, etc.
- Present Exhibits Side-By-Side
- “Tear Out” a Document Section to Create Focus
- Highlight On Command
- Manage Lots Of Exhibits And Have Them Ready To Go On Demand

Trial Presentation Programs

- Computer Based Solutions
  - Most Court Rooms Setup For Computers
  - Size Of Case Does Not Matter
  - Can Have Multiple Backs Of Exhibits On Hard Drives
  - Helps Create Exhibit Lists
  - Overlay Exhibits
  - Trial Director (InData Product)
    - Most Commonly Used Program
    - Database Program Which May Make It Harder To Learn Initially
    - Have To Learn How To Load Files
    - Can Support PDF & Native Files
    - Has An iPad Program Too
    - Single-User Licenses Start at $695, plus yearly subscription rates
    - Trial Director Has A Trial Version
  - Sanction (LexisNexis Product)
    - Less Commonly Used

Trial Director

What you see on your screen...

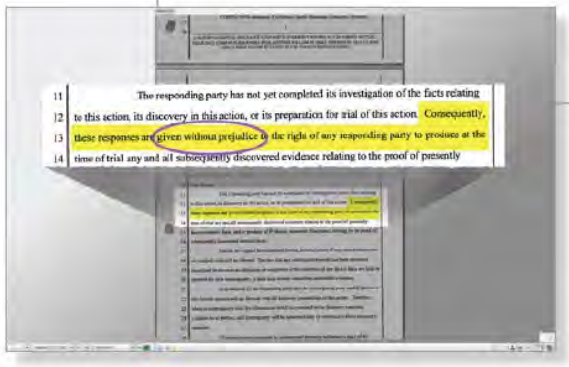


What they see on their screen...

DiMuroGinsberg PC
ATTORNEYS AT LAW

> *TrialDirector is simple to learn and simple to use. A 'must have' for any attorney who prefers to pay attention during trial instead of fumbling for his next exhibit.*

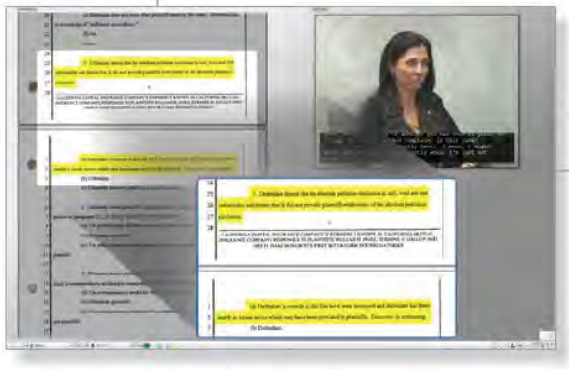
Michael Lee, Esquire
Michael Lee & Associates



Document in Presentation Mode

> *Holland & Hart has been using TrialDirector for over ten years now. The results have been several multi-million dollar wins in both plaintiff and defense work.*

Pen Volkman
Director of Graphics
& Video Services
Persuasion Strategies,
A Service of Holland & Hart



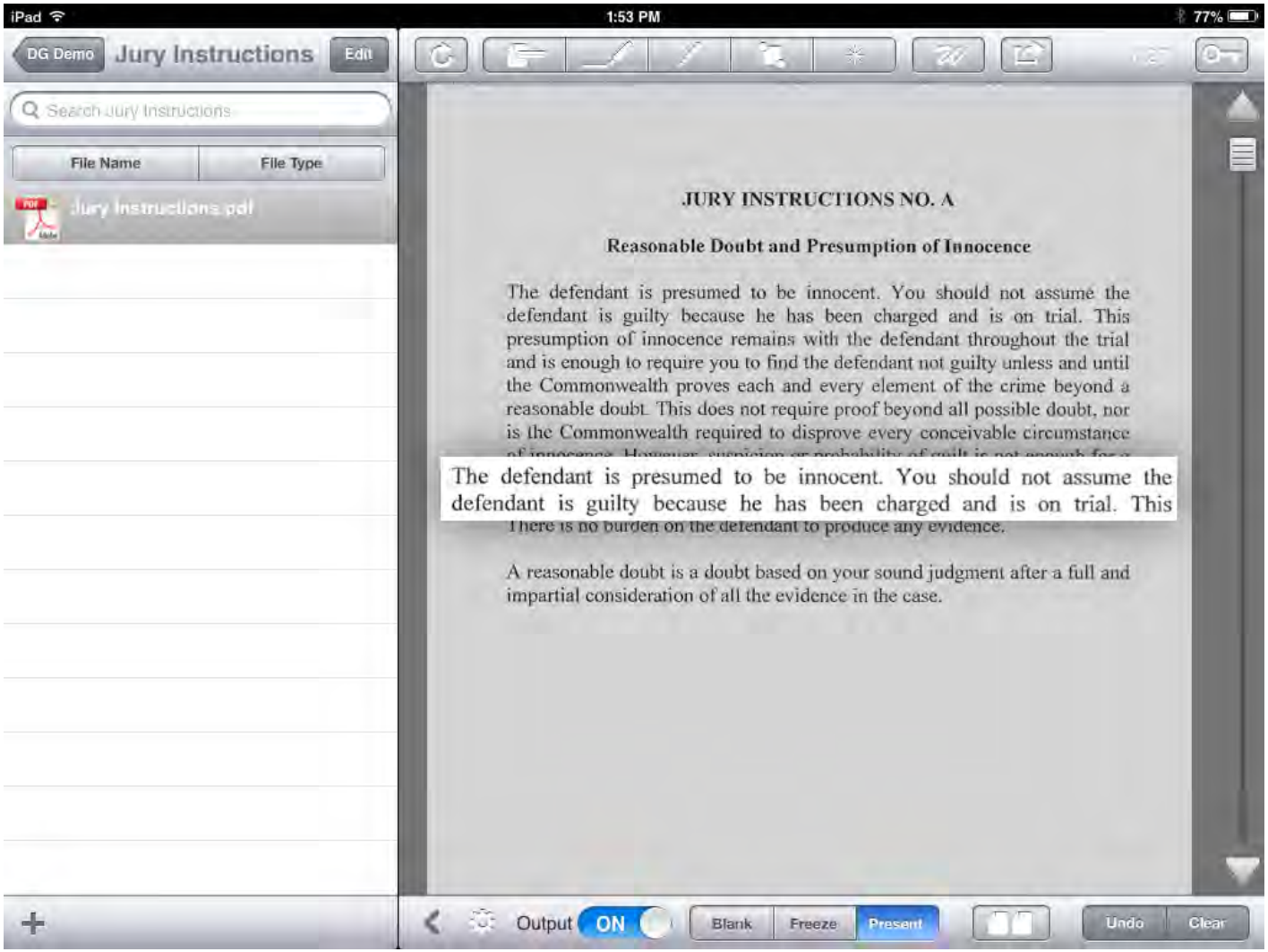
Witness Video in Presentation Mode

DiMuroGinsberg PC
ATTORNEYS AT LAW

Trial Presentation Software

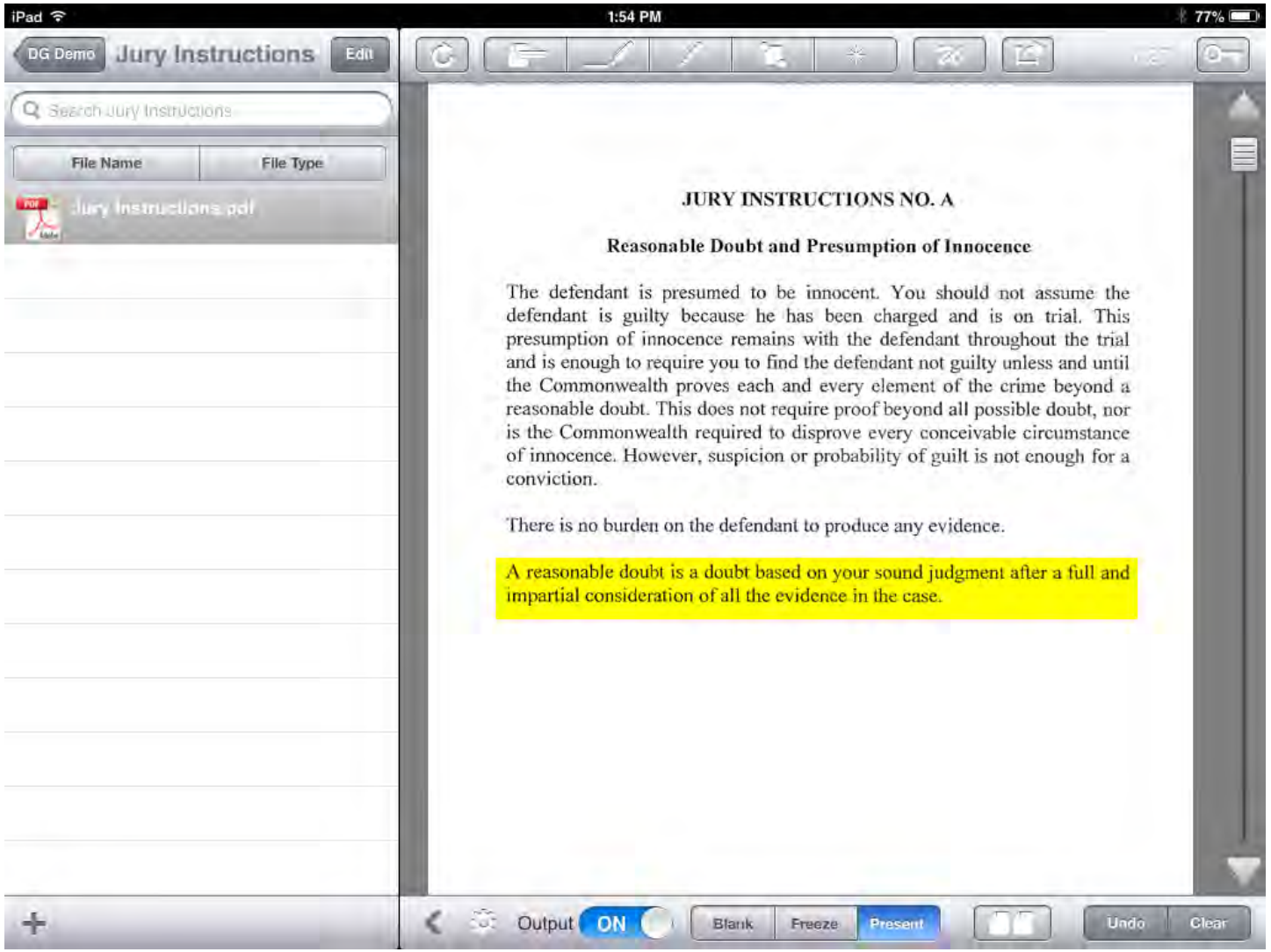
- iPad Based Solutions
  - Ease of Use
  - Cost Effective
  - Helps Organize and Create Exhibits
  - Inter-Active to Suit the Needs on the Spot
  - Mobile
  - TrialPad
    - One-time $90 for the App
    - Supports PDF, images (such as JPEG) and audio/video.
    - Does not support other native documents such as .ppt, .docx, .xl
    - Video Such as MP4 Must Be Converted Into iPad Supported Format
    - Need to Learn How to Download the Program

- "Tear Out" Capability



DiMuroGinsberg PC
ATTORNEYS AT LAW

Hi-Lighting Capability



DiMuroGinsberg PC
ATTORNEYS AT LAW

Edit Movies

DiMuroGinsberg PC
ATTORNEYS AT LAW

Trial Director v. Trial Pad

TRIAL DIRECTOR

PROS:
- Courtroom Adoptable
- Overlay Exhibits
- Support Native Files
- Comes with iPad App
- Flexible & Faster

CONS:
- Expensive ($695 per user)
- Requires Initial Learning Time
- Will Require 2nd Person for Tech Support/Presentation

TRIAL PAD

PROS:
- Cost Effective ($80)
- Mobile (can potentially be done by 1 attorney)
- White Board to make presentation more interactive
- Exhibit/Video Editing Capability

CONS:
- Courtroom Adoption is Not Guaranteed
- Does not support Native Files
- DropBox Dependent
- Requires Practice to Build Confidence

Service of Process Addresses

The information provided below comes directly from the respective provider's websites. At the conclusion of each provider's section, the source of the material is identified. For example, for Facebook the following is identified:

Source: https://www.facebook.com/safety/groups/law/guidelines/

This information is subject to change at any time and without notice by the providers. Do not rely upon the information contain here. Make sure to check directly with the provider before attempting to issue any subpoena.

Facebook

"US Legal Process Requirements
We disclose account records solely in accordance with our terms of service and applicable law, including the federal Stored Communications Act ("SCA"), 18 U.S.C. Sections 2701-2712. Under US law:

- A valid subpoena issued in connection with an official criminal investigation is required to compel the disclosure of basic subscriber records (defined in 18 U.S.C. Section 2703(c)(2)), which may include: name, length of service, credit card information, email address(es), and a recent login/logout IP address(es), if available.
- A court order issued under 18 U.S.C. Section 2703(d) is required to compel the disclosure of certain records or other information pertaining to the account, not including contents of communications, which may include message headers and IP addresses, in addition to the basic subscriber records identified above.
- A search warrant issued under the procedures described in the Federal Rules of Criminal Procedure or equivalent state warrant procedures upon a showing of probable cause is required to compel the disclosure of the stored contents of any account, which may include messages, photos, videos, wall posts, and location information.
- We interpret the national security letter provision as applied to Facebook to require the production of only 2 categories of information: name and length of service.

Submission of Requests
Online
Law enforcement officials may use the Law Enforcement Online Request System at facebook.com/records for the submission, tracking and processing of requests.

Please note that a government-issued email address is required to access the Law Enforcement Online Request System. You may also submit requests by email or fax as indicated below.

Email
records@fb.com

Fax
United States: +1 650 472-8007
Ireland: +353 (0)1 653 5373

Mail
United States Mail Address: 1601 Willow Road, Menlo Park CA 94025 Ireland
Mail Address: Hanover Reach | 5-7 Hanover Quay, | Dublin 2

Attention: Facebook Security, Law Enforcement Response Team
Law enforcement officials who do not submit requests through the Law Enforcement Online Request System at facebook.com/records should expect longer response times.

Notes

- Acceptance of legal process by any of these means is for convenience and does not waive any objections, including lack of jurisdiction or proper service.
- We will not respond to correspondence sent by non-law enforcement officials to the addresses above."

Source: https://www.facebook.com/safety/groups/law/guidelines/

LinkedIn

"User Agreement
9.3. Notices and Service of Process
In addition to Section 2.8. ("Notices and Service Messages"), we may notify you via postings on www.linkedin.com, www.slideshare.net or another LinkedIn site or app. You may contact us here. Or via mail or courier at: LinkedIn Corporation ATTN: Legal Department 2029 Stierlin Court Mountain View, CA 94043 USA Additionally, LinkedIn accepts service of process at this address. Any notices that you provide without compliance with this section shall have no legal effect."

Source: https://www.linkedin.com/legal/user-agreement

Instagram

"Information for Law Enforcement
Requests for User Information

We disclose account records solely in accordance with our terms of service and applicable law, including the federal Stored Communications Act ("SCA"), 18 U.S.C. Sections 2701-2712. Under the SCA:

- a valid subpoena issued in connection with an official criminal investigation is required to compel the disclosure of basic subscriber records (defined in 18 U.S.C. Section 2703(c)(2)), which may include: subscriber name, phone number, account creation date, email address, and a signup IP address, if available.
- a court order issued under 18 U.S.C. Section 2703(d) is required to compel the disclosure of certain records or other information pertaining to the account, not including contents of communications, which may include photographs, photo captions, and other electronic communication information in addition to the basic subscriber records identified above.
- a search warrant issued under the procedures described in the Federal Rules of Criminal Procedure or equivalent State warrant procedures upon a showing of probable cause is required to compel the disclosure of the stored contents of any account, which may include messages, photos, comments, and location information.

It is important to note that some information we store is collected automatically, while other information is provided by the user, and that we do not require email or identity verification. If a user has created a fake or anonymous profile, our information may not be authentic. We are unable to process overly broad or vague requests.

For reference, please read our Privacy Policy and Terms of Use.

Data Retention and Availability

We retain different types of information for different time periods. Given the volume of real-time content on Instagram, some information may only be stored for a short period of time. We do not retain data for law enforcement purposes unless we receive a valid preservation request. Preservation requests must include the username of the Instagram account in question, a valid return email address, and must be signed and sent on law enforcement letterhead.

Information to Include

All requests must identify the following:

1. The name of the issuing authority, badge/ID number of responsible agent, email address from a law enforcement domain, and a direct contact phone number.
2. The username of the Instagram account in question and details regarding specific information requested and its relationship to your investigation.
3. If you have access to an image's short URL, you can locate the username[.]
4. If you have access to the Instagram application, you can locate the username here:

Emergency Requests

Matters involving anticipated harm to a child or risk of death or serious physical injury to any person that requires disclosure of information without delay should contact us at lawenforcement@instagram.com.

It is important to note that we will not review or respond to messages sent to this email address by non-law enforcement officials. If you are a user aware of an emergency situation, you should immediately and directly contact local law enforcement officials.

Contact Information

Law enforcement officers may submit all records requests by email or mail.

Only email from law enforcement domains will be accepted. All others will be disregarded. Non-law enforcement requests should be sent through our regular support methods via Instagram's Help Center.

Email: lawenforcement@instagram.com

Mail:
Attn: Instagram Law Enforcement Response Team
1601 Willow Road
Menlo Park, CA 94025”

Source: http://help.instagram.com/494561080557017/

Twitter

“Requests for Twitter Account Information
Requests for user account information from U.S. law enforcement should be directed to Twitter, Inc. in San Francisco, California. Twitter responds to valid legal process issued in compliance with U.S. law.

Private Information Requires a Subpoena or Court Order

Non-public information about Twitter users will not be released to law enforcement except in response to appropriate legal process such as a subpoena, court order, or other valid legal process – or in response to a valid emergency request, as described below.

Contents of Communications Requires a Search Warrant
Requests for the contents of communications (e.g., Tweets, Direct Messages, photos) require a valid search warrant from an agency with proper jurisdiction over Twitter.

Will Twitter Notify Users of Requests for Account Information?
Yes. Twitter's policy is to notify users of requests for their account information, which includes a copy of the request, prior to disclosure unless we are prohibited from doing so (e.g., an order under 18 U.S.C. § 2705(b)). Exceptions may include exigent or counterproductive circumstances (e.g., emergencies; account compromises).

What Details Must Be Included in Account Information Requests?
When requesting user account information, please include:

- The @username and URL of the subject Twitter account in question (e.g., @safety and https://twitter.com/safety);
- Details about what specific information is requested (e.g., basic subscriber information) and its relationship to your investigation;
    - NOTE: Please ensure that the information you seek is not available from our public API. We are unable to process overly broad or vague requests.
- A valid official email address (e.g., name@agency.gov) so we may get back in touch with you upon receipt of your legal process.

Requests may be submitted by fax or mail; our contact information is available at the bottom of these Guidelines. Requests must be made on law enforcement letterhead. NOTE: We do not accept legal process via email at this time; our support system does not allow attachments for security reasons.

Production of Records
Unless otherwise agreed upon, we currently provide responsive records in electronic format (i.e., text files that can be opened with any word processing software such as Word or TextEdit).

Records Authentication
The records that we produce are self-authenticating. Additionally, the records are electronically signed to ensure their integrity at the time of production. If you require a declaration, please explicitly note that in your request.

<u>Emergency Disclosure Requests</u>
In line with our Privacy Policy, we may disclose account information to law enforcement in response to a valid emergency disclosure request.

Twitter, Inc. evaluates emergency disclosure requests on a case-by-case basis in compliance with relevant U.S. law (e.g., 18 U.S.C. § 2702(b)(8)). If we receive information that provides us with a good faith belief that there is an exigent emergency

involving the danger of death or serious physical injury to a person, we may provide information necessary to prevent that harm, if we have it.

How To Make an Emergency Disclosure Request
If there is an exigent emergency that involves the danger of death or serious physical injury to a person that Twitter may have information necessary to prevent, law enforcement officers can submit an emergency disclosure request through our web form (the quickest and most efficient method).

Alternatively, you may fax emergency requests to 1-415-222-9958 (faxed requests may result in a delayed response); please include all of the following information:

- Indication on your cover sheet, which must be on law enforcement letterhead, that you're submitting an Emergency Disclosure Request;
- Identity of the person who is in danger of death or serious physical injury;
- The nature of the emergency (e.g., report of suicide, bomb threat);
- Twitter @username and URL (e.g., @safety and https://twitter.com/safety) of the subject account(s) whose information is necessary to prevent the emergency;
- Any specific Tweets you would like us to review;
- The specific information requested and why that information is necessary to prevent the emergency;
- The signature of the submitting law enforcement officer;
- and All other available details or context regarding the particular circumstances.

International law enforcement authorities may submit requests for emergency disclosure.

Mutual Legal Assistance Treaties
Twitter, Inc.'s policy is to promptly respond to requests that are issued via U.S. court either by way of a mutual legal assistance treaty ("MLAT") and letters rogatory, upon proper service of process.

Assisting a Twitter User
If you are assisting a Twitter user with an investigation and want to obtain a copy of the Twitter user's non-public account information, please ask the user to contact us directly (see below) to request his or her own information.

Twitter Archive
Registered Twitter account holders can obtain a download of Tweets posted to their Twitter account. Directions on how a user can request that information is available in our Help Center.

Non-Public Information
Twitter does not currently offer account holders a self-serve method to obtain other, non-public information (e.g., IP logs) about their Twitter accounts. If a Twitter user requires his or her non-public account information, please direct the user to request this information directly from Twitter, Inc. by sending an email to privacy@twitter.com with subject: Request for Own Account Information; we will respond with further instructions.

Other Issues
Most issues can be resolved by having Twitter account holders submit inquires directly to us through our Help Center. More information on how to report violations is available here.

General Inquiries
Other general inquiries from law enforcement or government officials can be submitted through our web form.

Contact Information
Our address and fax details are:
Twitter, Inc.
c/o Trust & Safety - Legal Policy
1355 Market Street, Suite 900
San Francisco, CA 94103
Fax: 1-415-222-9958 (attn: Trust & Safety - Legal Policy)

Receipt of correspondence by any of these means is for convenience only and does not waive any objections, including the lack of jurisdiction or proper service."

Source: https://support.twitter.com/articles/41949-guidelines-for-law-enforcement#8

AT&T

"As part of the One AT&T corporate initiative, the AT&T Mobility subpoena function has been in a state of transition from North Palm Beach, FL to Dallas, TX for the past year. Effective March 1, 2011, the final phase of this process will be implemented.

Mobility subpoenas should be addressed to AT&T and submitted to:

AT&T Subpoena Center
208 S. Akard St., 10th Floor M
Dallas, TX 75202

Contact Number: (800) 291-4952
Fax: (877) 971-6093

Hours of Operation: Monday – Friday 8:00 am – 5:00 pm CT

Additional AT&T Contact Information
The website below provides general information related to the landline subpoena process and also facilitates an online process whereby landline subpoenas can be submitted.

Please do not use the website below for Mobility subpoenas, this will delay the return of records requested.

www.att.com/subpoena

Subpoena requests for AT&T Internet Services, Inc. should be directed to:

AT&T Internet Services Legal Compliance Group
1010 N. St. Mary's Street Room 315-A2
San Antonio, TX 78215

Contact: (210) 351-5219
Fax: (707) 435-6409

The AT&T National Compliance Center in North Palm Beach, Florida, will retain responsibility for all Mobility Court Orders, 911, and other legal process compliance work functions.

AT&T National Compliance Center
11760 US Highway One Mailstop: Suite 600
North Palm Beach, FL 33408

Contact: 800 - 635 - 6840
Fax #: 888 - 938 - 4715"

Source: http://info.publicintelligence.net/ATT-MobilitySubpoena.pdf

Sprint / Nextel

Subpeona Compliance Center
Sprint/Nextel
6480 Sprint Parkway
Overland Park, KS 66251
Contact: (800) 877-7330
Fax: (816) 600-3111

Virgin Mobile prepaid service = Sprint
Boost Mobile prepaid service = Nextel

After regular business hours call Sprint Subpoena Compliance Immediate Response Team at (855) 560-7690.

Verizon

"Legal Process Compliance
Responds to lawful process of business information, customer telephone and IP information.
Ensures court orders, search warrants, subpoenas and other legal document requests are processed confidentially and in compliance with all applicable laws.
Coordinates court appearances for Verizon Custodian of Records.

Contact Number
1-888-483-2600

Fax Number
325-949-6916

Mailing Address
Verizon Legal Compliance
Custodian of Record TXD01613
P.O. Box 1001
San Angelo, TX 76902

Hours of Operation
Monday - Friday 8:00 a.m. - 4:30 p.m."

Source:
http://www.verizon.com/Support/Residential/Phone/Homephone/General+Support/Support+Tools/General/122857.htm

T-Mobile

"Law Enforcement Relations
Role
The T-Mobile USA, Inc. Law Enforcement Relations Group (LER Group) is committed to efficiently assisting the law enforcement community with all lawfully authorized activities. Our Law Enforcement Relations unit is staffed by personnel who are well acquainted with the technical and evidentiary needs of federal, state, and local prosecutors and investigative officers. The unit maintains their proactive philosophy by offering educational presentations, reference materials and expedient, secure procedures that support the mission of the public safety community in an unparalleled fashion. Responsibilities of the LER Group include the following:

Responsibilities
- Processing lawful requests for subscriber identification information and historical billing data
- Providing technical assistance in the conduct of Lawfully Authorized Electronic Surveillance

- Testify as a custodian of records
- Ensuring company technical and procedural compliance with the federal Communications Assistance for Law Enforcement Act requirements
- Providing education to law enforcement regarding T-Mobile's GSM technology

T-Mobile USA Inc.
4 Sylvan Way
Parsippany, NJ 07054

Contact Information
Phone
(973) 292-8911

Fax
(973) 292-8697"

Source: http://www.t-mobile.com/Cms/Files/Published/0000BDF20016F5DD010312E2BDE4AE9B/0000BDF20016F5DE011CB9630A8D07DE/file/Law%20Enforcement%20Security%20Procedures%20For%20T-Mobile%20Website.pdf

Yahoo!

"COMPLIANCE GUIDE AT A GLANCE
How do I contact Yahoo! Legal?
Questions:
Compliance Team
Yahoo! Inc.
701 First Avenue
Sunnyvale, California 94089
408-349-3687 (tel.)

Subpoenas/Other Service of Process:
Fax requests for documents to Custodian of Records at 408-349-7941. Subpoenas for in person testimony must be personally served.

After-hours emergencies:
Yahoo! Security at 408-349-5400

General Tips:
- Include Yahoo! ID or Yahoo! email address in your request.
- Before making a request, check to see if the information sought is publicly available. See
- http://help.yahoo.com to find publicly available information.
- Make requests as specific and narrowly tailored as possible.

What Information Can Yahoo! Provide?

Subscriber Information

- Subscriber information supplied by the user at the time of registration, including name,
- location, date account created, and services used.
- IP addresses associated with log-ins to a user account are available for up to one year.
- Registration IP address data available for IDs registered since 1999.

Yahoo! Mail (including email associated with specific properties such as Personals, Small Business, Domains, and Flickr)

Any email available in the user's mail account, including IP address of computer used to send email.

Yahoo! is not able to search for or produce deleted emails.

Note that Yahoo! now hosts two new email domains: ymail.com and rocketmail.com.

Yahoo! Chat/Messenger

- Friends List for Yahoo! Messenger.
- Time, date, and IP address logs for Chat and Messenger use within the prior 45-60 days.
- Archives of Messenger communications may be available on the user's computer if the user has chosen to archive communications.
- Archives of Web Messenger communications may be stored on Yahoo! servers if at least one party to the communication chose to archive communications.

Yahoo! Groups

- Member list, email addresses of members, and date when members joined the Group.
- Information about Group moderators.
- Contents of the Files, Photos, and Messages sections.
- Group activity log describing when members subscribe and unsubscribe, post or delete files, and similar events.
- Note: Message Archive does not contain attachments to messages.

Yahoo! GeoCities, Domains, Web-hosting, and Stores

Active files user has uploaded to the website and date of file upload.

For stores, may have store transactional data.

Yahoo! Flickr

Contents in Flickr account and comments on other users' photos.

IP address and timestamp of content uploaded to account.

Flickr Groups to which a user belongs and Group content.

Yahoo! Profiles

Contents of a user's profile.

Time, date, and IP address logs of content added.

Does Yahoo! partner with other companies?

- Yahoo! has a co-branded service with AT&T. For customers with email addresses that have an SBC or AT&T suffix, AT&T has the primary customer relationship. In such cases, it is most appropriate to direct legal process first to AT&T.
- Yahoo! also has partnerships with Verizon, Rogers (Canada), and BT (UK).

Will Yahoo! preserve information?

- Yahoo! will preserve subscriber/customer information for 90 days. Yahoo! will preserve information for an additional 90-day period upon receipt of a request to extend the preservation.
- If Yahoo! does not receive formal legal process for the preserved information before the end of the preservation period, the preserved information may be deleted when the preservation period expires."

Source: http://cryptome.org/isp-spy/yahoo-spy.pdf

Google (Gmail)

"Address:
1600 Amphitheatre Parkway
Mountain View, CA 94043

Phone: (650) 623-4000
Fax: (650) 649-2939"

Source: http://www.criminaldivision.com/articles/39492/1/GOOGLE-E-MAIL-GMAIL---LEGAL-COMPLIANCE---SUBPOENA-COMPLIANCE-.html

AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 10-457 **August 5, 2010**
Lawyer Websites

Websites have become a common means by which lawyers communicate with the public. Lawyers must not include misleading information on websites, must be mindful of the expectations created by the website, and must carefully manage inquiries invited through the website. Websites that invite inquiries may create a prospective client-lawyer relationship under Rule 1.18. Lawyers who respond to website-initiated inquiries about legal services should consider the possibility that Rule 1.18 may apply.[1]

I. Introduction

Many lawyers and law firms have established websites as a means of communicating with the public. A lawyer website can provide to anyone with Internet access a wide array of information about the law, legal institutions, and the value of legal services. Websites also offer lawyers a twenty-four hour marketing tool by calling attention to the particular qualifications of a lawyer or a law firm, explaining the scope of the legal services they provide and describing their clientele, and adding an electronic link to contact an individual lawyer.

The obvious benefit of this information can diminish or disappear if the website visitor misunderstands or is misled by website information and features. A website visitor might rely on general legal information to answer a personal legal question. Another might assume that a website's provision of direct electronic contact to a lawyer implies that the lawyer agrees to preserve the confidentiality of information disclosed by website visitors.

For lawyers, website marketing can give rise to the problem of unanticipated reliance or unexpected inquiries or information from website visitors seeking legal advice. This opinion addresses some of the ethical obligations that lawyers should address in considering the content and features of their websites.[2]

II. Website Content

A. Information about Lawyers, their Law Firm, or their Clients

Lawyer websites may provide biographical information about lawyers, including educational background, experience, area of practice, and contact information (telephone, facsimile and e-mail address). A website also may add information about the law firm, such as its history, experience, and areas of practice, including general descriptions about prior engagements. More specific information about a lawyer or law firm's former or current clients, including clients' identities, matters handled, or results obtained also might be included.

Any of this information constitutes a "communication about the lawyer or the lawyer's services," and is therefore subject to the requirements of Model Rule 7.1[3] as well as the prohibitions against false and misleading statements in Rules 8.4(c) (generally) and 4.1(a) (when representing clients). Together, these rules prohibit false, fraudulent or misleading statements of law or fact. Thus, no website communication may be false or misleading, or may omit facts such that the resulting statement is materially misleading. Rules 5.1 and 5.3 extend this obligation to managerial lawyers in law firms by obligating them to make reasonable efforts to ensure the firm has in place measures giving reasonable assurance that all firm lawyers and nonlawyer assistants will comply with the rules of professional conduct.

---

[1] This opinion is based on the ABA Model Rules of Professional Conduct as amended by the ABA House of Delegates through August 2010. The laws, court rules, regulations, rules of professional conduct, and opinions promulgated in individual jurisdictions are controlling.

[2] We do not deal here with website content generated by governmental lawyers or offices or by non-profit law advocacy firms or organizations. *See, e.g., In re Primus*, 436 U.S. 412 (1978) (discussing how solicitation of prospective litigants by nonprofit organizations that engage in litigation as form of political expression and political association constitutes expressive and associational conduct entitled to First Amendment protection, which government may regulate only narrowly).

[3] *See, e.g.*, Arizona State Bar Op. 97-04 (1997), *available at* http://www.myazbar.org/Ethics/opinionview.cfm?id=480; California Standing Committee on Prof'l Resp. and Conduct Formal Op. 2001-155, 2001 WL 34029609 (2001); Hawaii Sup. Ct. Disc. Bd. Formal Op. 41 (2001), available at http://www.odchawaii.com/FORMAL_WRITTEN_OPINIONS.html; South Carolina Bar Eth. Advisory Committee Op. 04-06, 2004 WL 1520110 *1 (2004); Vermont Advisory Eth. Op. 2000-04, *available at* http://www.vtbar.org/Upload%20Files/WebPages/Attorney%20Resources/aeopinions/Advisory%20Ethics%20Opinions/Advertising/advertising.htm. Many state and local ethics opinions are published online can be accessed through the ABA Center for Professional Responsibility website at http://www.abanet.org/cpr/links.html.

As applied to lawyer websites, these rules allow a lawyer to include accurate information that is not misleading about the lawyer and the lawyer's law firm, including contact information and information about the law practice.[4] To avoid misleading readers, this information should be updated on a regular basis.[5] Specific information that identifies current or former clients or the scope of their matters also may be disclosed, as long as the clients or former clients give informed consent[6] as required by Rules 1.6 (current clients) and 1.9 (former clients).[7] Website disclosure of client identifying information is not normally impliedly authorized because the disclosure is not being made to carry out the representation of a client, but to promote the lawyer or the law firm.[8]

B. Information about the Law

Lawyers have long offered legal information to the public in a variety of ways, such as by writing books or articles, giving talks to groups, or staffing legal hotlines. Lawyer websites also can assist the public in understanding the law and in identifying when and how to obtain legal services.[9] Legal information might include general information about the law applicable to a lawyer's area(s) of practice, as well as links to other websites, blogs, or forums with related information. Information may be presented in narrative form, in a "FAQ" (frequently asked questions) format, in a "Q & A" (question and answer) format, or in some other manner.[10]

Legal information, like information about a lawyer or the lawyer's services, must meet the requirements of Rules 7.1, 8.4(c), and 4.1(a). Lawyers may offer accurate legal information that does not materially mislead reasonable readers.[11] To avoid misleading readers, lawyers should make sure that legal information is accurate and current,[12] and should include qualifying statements or disclaimers that "may preclude a finding that a statement is likely to create unjustified expectations or otherwise mislead a prospective client."[13] Although no exact line can be drawn between legal information and legal advice, both the context and content of the information offered are helpful in distinguishing between the two. [14]

---

[4] *See, e.g.*, North Carolina State Bar Formal Eth. Op. 2009-6 (2009) (firm may provide case summaries on website, including accurate information about verdicts and settlements, as long as it adds specific information about factual and legal circumstances of cases ((complexity, whether liability or damages were contested, whether opposing party was represented by counsel, firm's success in collecting judgment)) in conjunction with appropriate disclaimer to preclude misleading prospective clients).

[5] *See, e.g.*, Missouri Bar Inf. Advisory Op. 20060005 (2006) (firm must remove lawyer's biographical information within reasonable time after lawyer leaves firm).

[6] *See, e.g.*, Ohio Advisory Op. 2000-6, 2000 WL 1872572 *5 (2000) (law firm may list client's name on firm website with client's informed consent). *See also* New York Rule of Professional Conduct 7.1(b) (2) (2009) (lawyer may advertise name of regularly represented client, provided that client has given prior written consent).

[7] These rules apply to "all information relating to the representation, whatever its source" including publicly available information. Model Rule 1.6 cmt. 3. The consent can be oral or written. Rules 1.6 and 1.9(c) require informed consent, but do not require a written confirmation.

[8] *See* ABA Committee on Eth. and Prof'l Responsibility, Formal Op. 09-455 (2009) (Disclosure of Conflicts Information When Lawyers Move Between Law Firms) (absent demonstrable benefit to client's representation, disclosure of client identifying information, including client's name and nature of matter handled, is not impliedly authorized under Rule 1.6(a)).

[9] Model Rule 7.2 Comment [1] acknowledges that the "public's need to know about legal services can be fulfilled in part through advertising," a need that may be "particularly acute" in the case of persons who have not made extensive use of, or fear they may not be able to pay for, legal services.

[10] *See, e.g.*, Vermont Advisory Eth. Op. 2000-04, *supra* note 3 (lawyer may use "frequently asked questions" format as long as information is current, accurate, and includes clear statement that it does not constitute legal advice and readers should not rely on it to solve individual problem).

[11] Rule 7.1 Comment [2] provides that a "truthful statement is also misleading if there is a substantial likelihood that it will lead a reasonable person to formulate a specific conclusion ... for which there is no reasonable factual foundation."

[12] ABA Law Practice Management Section, *Best Practice Guidelines for Legal Information Web Site Providers* 1 (Feb. 2003), *available at* http://meetings.abanet.org/webupload/commupload/EP024500/relatedresources/best_practice_guidelines.pdf (website providing legal information should provide full and accurate information about identity and contact details of provider on each page of website, as well as dates on which substantive content was last reviewed).

[13] Model Rule 7.1 cmt. 3. *See, e.g.*, ABA Law Practice Management Section, *Best Practice Guidelines*, *supra* note 12 at 2 (website providers should avoid misleading users about jurisdiction to which site's content relates, and if clearly state-specific, the jurisdiction in which the law applies should be identified).

[14] *See, e.g.*, Arizona State Bar Op. 97-04, *supra* note 3 (because of inability to screen for conflicts of interest and possibility of disclosing confidential information, lawyers should not answer specific legal questions posed by laypersons in Internet chat rooms unless question presented is of general nature and advice given is not fact-specific); California Standing Committee on Prof'l Resp. and Conduct Formal Op. 2003-164, 2003 WL 23146203 (2003) (legal advice includes making recommendations about specific course of action to follow; public context of radio call-in show that includes warnings about information not being substitute for individualized legal advice makes it unlikely lawyers have agreed to act as caller's lawyer); South Carolina Bar Eth. Advisory Committee Op. 94-27 *2 (1995), 1995 WL 934127 (lawyer may maintain electronic presence for purpose of discussing legal topics, but must obtain sufficient information to make conflicts check before offering legal advice); Utah Eth. Op. 95-01 (1995), 1995 WL 49472 *1 ("how to" booklet on legal subject matter does not constitute practice of law).

With respect to context, lawyers who speak to groups generally have been characterized as offering only general legal information. With respect to content, lawyers who answer fact-specific legal questions may be characterized as offering personal legal advice, especially if the lawyer is responding to a question that can reasonably be understood to refer to the questioner's individual circumstances. However, a lawyer who poses and answers a hypothetical question usually will not be characterized as offering legal advice. To avoid misunderstanding, our previous opinions have recommended that lawyers who provide general legal information include statements that characterize the information as general in nature and caution that it should not be understood as a substitute for personal legal advice.[15]

Such a warning is especially useful for website visitors who may be inexperienced in using legal services, and may believe that they can rely on general legal information to solve their specific problem.[16] It would be prudent to avoid any misunderstanding by warning visitors that the legal information provided is general and should not be relied on as legal advice, and by explaining that legal advice cannot be given without full consideration of all relevant information relating to the visitor's individual situation.

C. Website Visitor Inquiries

Inquiries from a website visitor about legal advice or representation may raise an issue concerning the application of Rule 1.18 (Duties to Prospective Clients).[17] Rule 1.18 protects the confidentiality of prospective client communications. It also recognizes several ways that lawyers may limit subsequent disqualification based on these prospective client disclosures when they decide not to undertake a matter.[18]

Rule 1.18(a) addresses whether the inquirer has become a "prospective client," defined as "a person who discusses with a lawyer the possibility of forming a client-lawyer relationship."

---

[15] ABA Inf. Op. 85-1512 (1985) (Establishment of Private Multistate Lawyer Referral Service by Nonprofit Religious Organization), in FORMAL AND INFORMAL ETHICS OPINIONS: FORMAL OPINIONS 1983-1998, at 550, 551 (ABA 2000) (not unethical to prepare articles of general legal information for lay public, but may be prudent to include statement that information furnished is only general and not substitute for personalized legal advice); ABA Inf. Op. 85-1510 (1985) (Establishment of Multistate Private Lawyer Referral Service for Benefit of Subscribers to Corporation's Services), in FORMAL AND INFORMAL ETHICS OPINIONS: FORMAL OPINIONS 1983-1998, at 544, 545 (corporate counsel may author articles of general legal information for corporations' subscriber newsletter, but "good practice" to include a statement that information is only general in nature and not substitute for personal legal advice).

[16] *See, e.g.*, ABA Law Practice Management Section, *Best Practice Guidelines*, *supra* note 12 at 3 (websites that provide legal information should give users conspicuous notice that information does not constitute legal advice). Some state opinions also warn against providing specific or particularized facts in a lawyer's communication to avoid creating a client-lawyer relationship. *See also* District of Columbia Bar Eth. Op. 316 (2002), *available at* http://www.dcbar.org/for_lawyers/ethics/legal_ethics/opinions/opinion316.cfm (online chat rooms and listserves); Maryland State Bar Ass'n Committee on Eth. Op. 2007-18 (2008) (lawyer conducting domestic relations law seminars for lay public); New Jersey Advisory Committee on Prof'l Eth. Op. 712 (2008) (Attorney-Staffed Legal Hotline For Members of Nonprofit Trade Association), *available at* http://lawlibrary.rutgers.edu/ethics/acpe/acp712_1.html (lawyer staffing telephone hotline); New Jersey Advisory Committee on Prof'l Eth. Op 671, 1993 WL 137685 (1993) (Activities and Obligations of Pro Bono Attorneys), (lawyer-volunteer at abused women shelter); New Mexico Bar Op. 2001-1 (2001) (Application of Rules of Professional Conduct to Lawyer's Use of Listserve-type Message Boards and Communications) (listserves); Wisconsin Prof'l Eth. Committee Op. E-95-5 (1995), *available at* http://www.wisbar.org/AM/Template.cfm?Section=Legal_Research&Template=/CustomSource/Search/Search.cfm&output=xml_no_dtd&proxystylesheet=wisbar5&client=wisbar5&filter=1&start=0&Site=SBW&q=%22formal+opinion%22+E%2D95%2D5&submit=ethics (lawyer-volunteer at organization that provides information about landlord-tenant law). The Model Rules defer to "principles of substantive law external to these Rules [to] determine when a client-lawyer relationship exists." Scope cmt. 17.

[17] *See, e.g.*, Arizona State Bar Op. 02-04 (2002), *available at* http://www.myazbar.org/Ethics/opinionview.cfm?id=288 (lawyer does not owe duty of confidentiality to individuals who unilaterally e-mail inquiries to lawyer when e-mail is unsolicited); California Standing Committee on Prof'l Resp. and Conduct Formal Op. 2001-155, *supra* note 3 (lawyer may avoid incurring duty of confidentiality to persons who seek legal services by visiting lawyer's website and disclose confidential information only if site contains clear disclaimer); Iowa Bar Ass'n Eth. Op. 07-02 (2007), *available at* http://www.iowabar.org/ethics.nsf/e61beed77a215f6686256497004ce492/cb0a70672d69d8c1862573380013fb9d?OpenDocument (message that encourages detailed response about case could in some situations be considered bilateral); New Hampshire Bar Ass'n Eth. Committee Op. 2009-2010/1(2009), *available at* http://www.nhbar.org/legal-links/ethics1.asp (when law firm's website invites public to send e-mail to one of firm's lawyers, it is opening itself to potential obligations to prospective clients); Ass'n of the Bar of the City of New York, Formal Op. 2001-1 (2001) (Obligations Of Law Firm Receiving Unsolicited E-Mail Communications From Prospective Client), *available at* http://www.abcny.org/Ethics/eth2001-01.html (where firm website does not adequately warn that information transmitted will not be treated as confidential, information should be held in confidence by lawyer receiving communication and not disclosed to or used for benefit of another client even though lawyer declines to represent potential client); New Jersey Advisory Committee on Prof'l Eth. Op. 695, 2004 WL 833032 (2004) (firm has duty to keep information received from prospective client confidential); San Diego County Bar Ass'n Eth. Op. 2006-1 (2006), *available at* http://www.sdcba.org/index.cfm?Pg=ethicsopinion06-1 (private information received from non-client via unsolicited e-mail is not required to be held as confidential if lawyer has not had opportunity to warn or stop flow of information at or before the communication is delivered).

[18] Lawyers do not normally owe confidentiality obligations to persons who are not clients (protected by Rule 1.6), former clients (Rule 1.9), or prospective clients (Rule 1.18).

To "discuss," meaning to talk about, generally contemplates a two-way communication, which necessarily must begin with an initial communication.[19] Rule 1.18 implicitly recognizes that this initial communication can come either from a lawyer or a person who wishes to become a prospective client.

Rule 1.18 Comment [2] also recognizes that not all initial communications from persons who wish to be prospective clients necessarily result in a "discussion" within the meaning of the rule: "a person who communicates information unilaterally to a lawyer, without any reasonable expectation that the lawyer is willing to discuss the possibility of forming a client-lawyer relationship, is not a prospective client."

For example, if a lawyer website specifically requests or invites submission of information concerning the possibility of forming a client-lawyer relationship with respect to a matter, a discussion, as that term is used in Rule 1.18, will result when a website visitor submits the requested information.[20] If a website visitor submits information to a site that does not specifically request or invite this, the lawyer's response to that submission will determine whether a discussion under Rule 1.18 has occurred.

A telephone, mail or e-mail exchange between an individual seeking legal services and a lawyer is analogous.[21] In these contexts, the lawyer takes part in a bilateral discussion about the possibility of forming a client-lawyer relationship and has the opportunity to limit or encourage the flow of information. For example, the lawyer may ask for additional details or may caution against providing any personal or sensitive information until a conflicts check can be completed.

Lawyers have a similar ability on their websites to control features and content so as to invite, encourage, limit, or discourage the flow of information to and from website visitors.[22] A particular website might facilitate a very direct and almost immediate bilateral communication in response to marketing information about a specific lawyer. It might, for example, specifically encourage a website visitor to submit a personal inquiry about a proposed representation on a conveniently-provided website electronic form which, when responded to, begins a "discussion" about a proposed representation and, absent any cautionary language, invites submission of confidential information.[23] Another website might describe the work of the law firm and each of its lawyers, list only contact information such as a telephone number, e-mail or street address, or provide a website e-mail link to a lawyer. Providing such information alone does not create a reasonable expectation that the lawyer is willing to discuss a specific client-lawyer relationship.[24] A lawyer's response to an inquiry submitted by a visitor who uses this contact information may, however, begin a "discussion" within the meaning of Rule 1.18.

In between these two examples, a variety of website content and features might indicate that a lawyer has agreed to discuss a possible client-lawyer relationship. A former client's website communication to a lawyer about a new matter must be analyzed in light of their previous relationship, which may have given rise to a reasonable expectation of confidentiality.[25] But a person who knows that the lawyer already declined a particular representation or is already representing an adverse party can neither reasonably expect confidentiality, nor reasonably believe that

---

[19] For example, in ABA Committee on Eth. and Prof'l Responsibility, Formal Op. 90-358 (1990) (Protection of Information Imparted by Prospective Client), this Committee considered the obligations of a lawyer who engaged in such a "discussion" in the context of a face-to-face meeting.

[20] Rule 1.18 cmt. 1.

[21] *See, e.g.*, Virginia Legal Eth. Op. 1842 (2008), *available at* http://www.vacle.org/opinions/1842.htm (absent voicemail message that asks for detailed information, providing phone number and voicemail is an invitation only to contact lawyer, not to submit confidential information); Iowa State Bar Ass'n Eth. Op. 07-02 ("Communication from and with Potential Clients), *available at* http://www.iowabar.org/ethics.nsf/e61beed77a215f6686256497004ce492/cb0a70672d69d8c1862573380013fb9d?OpenDocument (telephone voicemail message that simply asks for contact details does not give rise to bilateral communication, but message that encourages caller to leave detailed messages about their case could be considered bilateral).

[22] *See, e.g.*, Arizona State Bar Op. 02-04 (2002), *available at* http://www.myazbar.org/Ethics/opinionview.cfm?id=288 (lawyers who maintain websites with e-mail links should include disclaimers to clarify whether e-mail communications from prospective clients will be treated as confidential); Massachusetts Bar Ass'n Op. 07-01 (2007), *available at* http://www.massbar.org/publications/ethics-opinions/2000-2009/2007/opinion-07-01 (lawyer who receives unsolicited information from prospective client through e-mail link on law firm website without effective disclaimer must hold information confidential because law firm has opportunity to set conditions on flow of information); South Dakota Bar Eth. Op. 2002-2 (2002) (lawyer's website that invites viewers to send e-mail through jump site creates expectation of confidentiality).

[23] *See, e.g.*, Iowa State Bar Ass'n Eth. Op. 07-02, *supra* note 21 (web page inviting specific questions constitutes bilateral communication with expectation of confidentiality) and Virginia Legal Eth. Op. 1842 *supra* note 21 (website that specifically invites visitor to submit information in exchange for evaluation invites formation of client-lawyer relationship).

[24] E-mails received from unknown persons who send them apart from the lawyer's website may even more easily be viewed as unsolicited. *See, e.g.*, Arizona State Bar Op. 02-04, *supra* note 22 (e-mail to multiple lawyers asking for representation); Iowa State Bar Ass'n Eth. Op. 07-02, *supra* note 21 (website that gives contact information does not without more indicate that lawyer requested or consented to sending of confidential information); San Diego County Bar Assn. Op. 2006-1, *available at* http://www.sdcba.org/index.cfm?Pg=ethicsopinion06-1 (inquirer found lawyer's e-mail address on state bar membership records website accessible to the public).

[25] *See, e.g.*, Iowa State Bar Ass'n Committee Eth. Op. 07-02, *supra* note 22 (lack of prior relationship with person sending unsolicited e-mail requesting representation was one factor in determining whether communicator's disclosures were unilateral and whether expectation of

the lawyer wishes to discuss a client-lawyer relationship. Similarly, a person who purports to be a prospective client and who communicates with a number of lawyers with the intent to prevent other parties from retaining them in the same matter should have no reasonable expectation of confidentiality or that the lawyer would refrain from an adverse representation.[26]

In other circumstances, it may be difficult to predict when the overall message of a given website communicates a willingness by a lawyer to discuss a particular prospective client-lawyer relationship. Imprecision in a website message and failure to include a clarifying disclaimer may result in a website visitor reasonably viewing the website communication itself as the first step in a discussion.[27] Lawyers are therefore well-advised to consider that a website-generated inquiry may have come from a prospective client, and should pay special attention to including the appropriate warnings mentioned in the next section.

If a discussion with a prospective client has occurred, Rule 1.18(b) prohibits use or disclosure of information learned during such a discussion absent the prospective client's informed consent.[28] When the discussion reveals a conflict of interest, the lawyer should decline the representation,[29] and cannot disclose the information received without the informed consent of the prospective client.[30] For various reasons, including the need for a conflicts check, the lawyer may have tried to limit the initial discussion and may have clearly expressed those limitations to the prospective client. If this has been done, any information given to the lawyer that exceeds those express limitations generally would not be protected under Rule 1.18(b).

Rule 1.18(c) disqualifies lawyers and their law firms who have received information that "could be significantly harmful" to the prospective client from representing others with adverse interests in the same or substantially related matters.[31] For example, if a prospective client previously had disclosed only an intention to bring a particular lawsuit and has now retained a different lawyer to initiate the same suit, it is difficult to imagine any significant harm that could result from the law firm proceeding with the defense of the same matter.[32] On the other hand, absent an appropriate warning, the prospective client's prior disclosure of more extensive facts about the matter may well be disqualifying.

Rule 1.18(d) creates two exceptions that allow subsequent adverse representation even if the prospective client disclosed information that was significantly harmful: (1) informed consent confirmed in writing from both the affected and the prospective client, or (2) reasonable measures to limit the disqualifying information, combined with timely screening of the disqualified lawyer from the subsequent adverse matter. Rule 1.18(d) (2) specifically would allow the law firm (but not the contacted lawyer) to "undertake or continue" the representation of someone with adverse interests without receiving the informed consent of the prospective client if the lawyer who initially received the information took reasonable precautions to limit the prospective client's initial disclosures and was timely screened from further involvement in the matter as required by Rule 1.0(k).

III. Warnings or Cautionary Statements Intended to Limit, Condition, or Disclaim a Lawyer's Obligations to Website Visitors

Warnings or cautionary statements on a lawyer's website can be designed to and may effectively limit, condition, or disclaim a lawyer's obligation to a website reader. Such warnings or statements may be written so as

---

confidentiality was reasonable); Oregon Eth. Op. 2005-146, 2005 WL 5679570 *1 (2005) (lawyer who sends periodic reminders to former clients risks giving recipients reasonable belief they are still current clients).

[26] *See, e.g.*, Virginia Legal Eth. Op. 1794 (2004), *available at* http://www.vacle.org/opinions/1794.htm (person who meets with lawyer for primary purpose of precluding others from obtaining legal representation does not have reasonable expectation of confidentiality); Ass'n of the Bar of the City of New York Committee on Prof'l and Jud. Eth. Formal Op. 2001-1 (2001), *available at* http://www.abcny.org/Ethics/eth2001.html ("taint shoppers," who interview lawyers or law firms for purpose of disqualifying them from future adverse representation, have no good faith expectation of confidentiality).

[27] *See e.g.*, Massachusetts Bar Ass'n Op. 07-01, *supra* note 22 (in absence of effective disclaimer, prospective client visiting law firm website that markets background and qualifications of each lawyer in attractive light, stresses lawyer's skill at solving clients' practical problems, and provides e-mail link for immediate communication with that lawyer might reasonably conclude that firm and its individual lawyers have implicitly "agreed to consider" whether to form client-lawyer relationship).

[28] Rule 1.18(b) allows disclosure or use if permitted by Rule 1.9. Rule 1.9(c) (2) and its Comment [7] in turn link disclosure to Rule 1.6, the general confidentiality rule, which requires client informed consent to disclosure.

[29] Rule 1.18 cmt. 4.

[30] Rule 1.18 cmt. 3.

[31] *See also* RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 15 (2) (2000).

[32] Rule 1.18 cmt. 5 also allows lawyers to condition an initial conversation on the prospective client's informed consent to subsequent adverse representation in the same matter or subsequent use of any confidential information provided.

to avoid a misunderstanding by the website visitor that (1) a client-lawyer relationship has been created;[33] (2) the visitor's information will be kept confidential;[34] (3) legal advice has been given;[35] or (4) the lawyer will be prevented from representing an adverse party.[36]

Limitations, conditions, or disclaimers of lawyer obligations will be effective only if reasonably understandable, properly placed, and not misleading. This requires a clear warning in a readable format whose meaning can be understood by a reasonable person.[37] If the website uses a particular language, any waiver, disclaimer, limitation, or condition must be in the same language. The appropriate information should be conspicuously placed to assure that the reader is likely to see it before proceeding.[38]

Finally, a limitation, condition, waiver, or disclaimer may be undercut if the lawyer acts or communicates contrary to its warning.

---

[33] *See, e.g.*, New Mexico Bar Op. 2001-1 (2001), *available at* http://www.nmbar.org/legalresearch/ethicsadvisoryopinions.html (appropriate disclaimers of attorney-client relationship should accompany any response to listserve message board, but any response that would suggest to reasonable person that, despite disclaimer, relationship is being or has been established, would negate disclaimer); North Carolina State Bar Formal Eth. Op. 2000-3, 2000 WL 33300702 *2 (2000) (Responding to Inquiries Posted on a Message Board on the Web) (lawyers who do not want to create client-lawyer relationships on law firm message board should use specific disclaimers on any communications with inquirers, but substantive law will determine whether client-lawyer relationship is created); Ass'n of the Bar of the City of New York Committee on Prof'l and Jud. Eth. Formal Op. 1998-2 (1998), *available at* http://www.abcny.org/Ethics/eth1998-2.htm (disclaimer that "if specific legal advice is sought, we will indicate that this requires establishment of an attorney-client relationship which cannot be carried out through the use of a web page" may not necessarily serve to shield law firm from claim that attorney-client relationship was established by specific on-line communications); Utah State Bar Eth. Advisory Op. Committee Op. 96-12, 1997 WL 45137 *1 (1997) ("if legal advice is sought from an attorney, if the advice sought is pertinent to the attorney's profession, and if the attorney gives the advice for which fees will be charged, an attorney-client relationship is created that cannot be disclaimed by the attorney giving the advice"); Vermont Bar Ass'n Advisory Eth. Op. 2000-04 (2000), *supra* note 3 (despite website caveat and disclaimers, nonlawyer may still rely on information on website or lawyer's responses; disclaimer cannot preclude possibility of establishing client-lawyer relationship in an individual case).

[34] The Committee does not opine whether a confidentiality waiver might affect the attorney-client privilege. *See, e.g.*, Barton v. U.S. Dist. Ct. for the Cent. Dist. of Cal., 410 F. 3d 1104, 1111-12 (9th Cir. 2005) (checking "yes" box on law firm website that acknowledged providing information in answer to questionnaire "does not constitute a request for legal advice and I am not forming an attorney-client relationship by submitting this information" did not waive attorney-client privilege because confidentiality was not mentioned in attempted disclaimer and questionnaires were nevertheless submitted in course of seeking attorney-client relationship in potential class action). *Cf.* Schiller v. The City of New York, 245 F.R.D. 112, 117-18 (S.D.N.Y. 2007) (although privilege may protect pre-engagement communications from prospective clients, it does not apply to person who completed questionnaires soliciting information from N.Y. Civil Liberties Union to allow it to "effectively advocate for change"). *See also* David Hricik, *To Whom it May Concern: Using Disclaimers to Avoid Disqualification by Receipt of Unsolicited E-Mail from Prospective Clients*, 16 ABA PROFESSIONAL LAWYER 1, 5 (2005) (agreement that waives all confidentiality tries to do too much and might destroy the ability of prospective client who eventually becomes firm client to claim privilege).

[35] *See* note 15 *supra.*

[36] Rule 1.18 cmt. 5.

[37] *See, e.g.*, California Bar Committee on Prof'l Resp. Op. 2005-168, 2005 WL 3068090 *4 (2005) (finding disclaimer stating that "confidential relationship" would not be formed was not enough to waive confidentiality, because it confused not forming client-lawyer relationship with agreeing to keep communications confidential).

[38] *See, e.g.*, District of Columbia Bar Eth. Op. 302 (2000), *available at* http://www.dcbar.org/for_lawyers/ethics/legal_ethics/opinions/opinion302.cfm (lawyers may want to use "click through" pages that automatically direct the reader to another webpage containing disclaimers to ensure that visitors are not misled and other devices such as confirmatory messages that clarify nature of relationship); Virginia Legal Eth. Op. 1842, *supra* note 21 (approving of prominent "click through" disclaimers that require readers to assent to terms of disclaimer before submitting information). Courts have refused to uphold disclaimers or licensing agreements that appeared on separate pages and did not require a reader's affirmative consent to their terms because they did not provide reasonable notice). *See, e.g.*, Sprecht v. Netscape Communications Corp., 306 F.3d 17, 31-32 (2d Cir. 2002). On the other hand, courts have upheld website restrictions that provided actual knowledge by presenting the information and requiring an affirmative action (a click through or "clickwrap" agreement) before gaining access to the website content. *See, e.g.*, Register.com v. Verio, 356 F.3d 393, 401-02 (2d Cir. 2004).

AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 11-459 **August 4, 2011**

Duty to Protect the Confidentiality of E-mail Communications with One's Client

A lawyer sending or receiving substantive communications with a client via e-mail or other electronic means ordinarily must warn the client about the risk of sending or receiving electronic communications using a computer or other device, or e-mail account, where there is a significant risk that a third party may gain access. In the context of representing an employee, this obligation arises, at the very least, when the lawyer knows or reasonably should know that the client is likely to send or receive substantive client-lawyer communications via e-mail or other electronic means, using a business device or system under circumstances where there is a significant risk that the communications will be read by the employer or another third party.[1]

Introduction

Lawyers and clients often communicate with each other via e-mail and sometimes communicate via other electronic means such as text messaging. The confidentiality of these communications may be jeopardized in certain circumstances. For example, when the client uses an employer's computer, smartphone or other telecommunications device, or an employer's e-mail account to send or receive e-mails with counsel, the employer may obtain access to the e-mails. Employers often have policies reserving a right of access to employees' e-mail correspondence via the employer's e-mail account, computers or other devices, such as smartphones and tablet devices, from which their employees correspond. Pursuant to internal policy, the employer may be able to obtain an employee's communications from the employer's e-mail server if the employee uses a business e-mail address, or from a workplace computer or other employer-owned telecommunications device on which the e-mail is stored even if the employee has used a separate, personal e-mail account. Employers may take advantage of that opportunity in various contexts, such as when the client is engaged in an employment dispute or when the employer is monitoring employee e-mails as part of its compliance responsibilities or conducting an internal investigation relating to the client's work.[2] Moreover, other third parties may be able to obtain access to an employee's electronic communications by issuing a subpoena to the employer. Unlike conversations and written communications, e-mail communications may be permanently available once they are created.

The confidentiality of electronic communications between a lawyer and client may be jeopardized in other settings as well. Third parties may have access to attorney-client e-mails when the client receives or sends e-mails via a public computer, such as a library or hotel computer, or via a borrowed computer. Third parties also may be able to access confidential communications when the client uses a computer or other device available to others, such as when a client in a matrimonial dispute uses a home computer to which other family members have access.

In contexts such as these, clients may be unaware of the possibility that a third party may gain access to their personal correspondence and may fail to take necessary precautions. Therefore, the risk that third parties may obtain access to a lawyer's e-mail communications with a client raises the question of what, if any, steps a lawyer must take to prevent such access by third parties from occurring. This opinion addresses this question in the following hypothetical situation.

An employee has a computer assigned for her exclusive use in the course of her employment. The company's written internal policy provides that the company has a right of access to all employees' computers and e-mail files, including those relating to employees' personal matters. Notwithstanding this

---

[1] This opinion is based on the ABA Model Rules of Professional Conduct as amended by the ABA House of Delegates through August 2011. The laws, court rules, regulations, rules of professional conduct, and opinions promulgated in individual jurisdictions are controlling.

[2] Companies conducting internal investigations often secure and examine the e-mail communications and computer files of employees who are thought to have relevant information.

policy, employees sometimes make personal use of their computers, including for the purpose of sending personal e-mail messages from their personal or office e-mail accounts. Recently, the employee retained a lawyer to give advice about a potential claim against her employer. When the lawyer knows or reasonably should know that the employee may use a workplace device or system to communicate with the lawyer, does the lawyer have an ethical duty to warn the employee about the risks this practice entails?

Discussion

Absent an applicable exception, Rule 1.6(a) requires a lawyer to refrain from revealing "information relating to the representation of a client unless the client gives informed consent." Further, a lawyer must act competently to protect the confidentiality of clients' information. This duty, which is implicit in the obligation of Rule 1.1 to "provide competent representation to a client," is recognized in two Comments to Rule 1.6. Comment [16] observes that a lawyer must "act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision." Comment [17] states in part: "When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients.... Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement."

This Committee has recognized that these provisions of the Model Rules require lawyers to take reasonable care to protect the confidentiality of client information,[3] including information contained in e-mail communications made in the course of a representation. In ABA Op. 99-413 (1999) ("Protecting the Confidentiality of Unencrypted E-Mail"), the Committee concluded that, in general, a lawyer may transmit information relating to the representation of a client by unencrypted e-mail sent over the Internet without violating Model Rule 1.6(a) because the mode of transmission affords a reasonable expectation of privacy from a technological and legal standpoint. The opinion, nevertheless, cautioned lawyers to consult with their clients and follow their clients' instructions as to the mode of transmitting highly sensitive information relating to the clients' representation. It found that particularly strong protective measures are warranted to guard against the disclosure of highly sensitive matters.

Clients may not be afforded a "reasonable expectation of privacy" when they use an employer's computer to send e-mails to their lawyers or receive e-mails from their lawyers. Judicial decisions illustrate the risk that the employer will read these e-mail communications and seek to use them to the employee's disadvantage. Under varying facts, courts have reached different conclusions about whether an employee's client-lawyer communications located on a workplace computer or system are privileged, and the law appears to be evolving.[4] This Committee's mission does not extend to interpreting the substantive law, and

---

[3] *See, e.g.*, ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 08-451 (2008) (Lawyer's Obligations When Outsourcing Legal and Nonlegal Support Services) ("the obligation to 'act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision'" requires a lawyer outsourcing legal work "to recognize and minimize the risk that any outside service provider may inadvertently -- or perhaps even advertently -- reveal client confidential information to adverse parties or to others who are not entitled to access ... [and to] verify that the outside service provider does not also do work for adversaries of their clients on the same or substantially related matters.").

[4] *See, e.g.*, Stengart v. Loving Care Agency, Inc., 990 A.2d 650, 663 (N.J. 2010) (privilege applied to e-mails with counsel using "a personal, password protected e-mail account" that were accessed on a company computer); Sims v. Lakeside Sch., No. C06-1412RSM, 2007 WL 2745367, at *2 (W.D. Wash. Sept. 20, 2007) (privilege applied to web-based e-mails to and from employee's counsel on hard drive of computer furnished by employer); National Econ. Research Assocs. v. Evans, No. 04–2618–BLS2, 21 Mass.L.Rptr. 337, 2006 WL 2440008, at *5 (Mass. Super. Aug. 3, 2006) (privilege applied to "attorney-client communications unintentionally stored in a temporary file on a company-owned computer that were made via a private, password-protected e-mail account accessed through the Internet, not the company's Intranet"); Holmes v. Petrovich Development Co., 191 Cal.App.4th 1047, 1068-72 (2011) (privilege

therefore we express no view on whether, and in what circumstances, an employee's communications with counsel from the employee's workplace device or system are protected by the attorney-client privilege. Nevertheless, we consider the ethical implications posed by the risks that these communications will be reviewed by others and held admissible in legal proceedings.[5] Given these risks, a lawyer should ordinarily advise the employee-client about the importance of communicating with the lawyer in a manner that protects the confidentiality of e-mail communications, just as a lawyer should avoid speaking face-to-face with a client about sensitive matters if the conversation might be overheard and should warn the client against discussing their communications with others. In particular, as soon as practical after a client-lawyer relationship is established, a lawyer typically should instruct the employee-client to avoid using a workplace device or system for sensitive or substantive communications, and perhaps for any attorney-client communications, because even seemingly ministerial communications involving matters such as scheduling can have substantive ramifications.

The time at which a lawyer has an ethical obligation under Rules 1.1 and 1.6 to provide advice of this nature will depend on the circumstances. At the very least, in the context of representing an employee, this ethical obligation arises when the lawyer knows or reasonably should know that the client is likely to send or receive substantive client-lawyer communications via e-mail or other electronic means,[6] using a business device or system under circumstances where there is a significant risk that the communications will be read by the employer or another third party. Considerations tending to establish an ethical duty to protect client-lawyer confidentiality by warning the client against using a business device or system for substantive e-mail communications with counsel include, but are not limited to, the following: (1) that the client has engaged in, or has indicated an intent to engage in, e-mail communications with counsel; (2) that the client is employed in a position that would provide access to a workplace device or system; (3) that, given the circumstances, the employer or a third party has the ability to access the e-mail communications; and (4) that, as far as the lawyer knows, the employer's internal policy and the jurisdiction's laws do not clearly protect the privacy of the employee's personal e-mail communications via a business device or system. Unless a lawyer has reason to believe otherwise, a lawyer ordinarily should assume that an employer's internal policy allows for access to the employee's e-mails sent to or from a workplace device or system.

The situation in the above hypothetical is a clear example of where failing to warn the client about the risks of e-mailing communications on the employer's device can harm the client, because the employment dispute would give the employer a significant incentive to access the employee's workplace e-mail and the employer's internal policy would provide a justification for doing so. The obligation arises once the lawyer has reason to believe that there is a significant risk that the client will conduct e-mail communications with the lawyer using a workplace computer or other business device or via the employer's e-mail account. This possibility ordinarily would be known, or reasonably should be known, at the outset of the representation. Given the nature of the representation–an employment dispute–the lawyer is on notice that the employer may search the client's electronic correspondence. Therefore, the lawyer must ascertain, unless the answer is already obvious, whether there is a significant risk that the client will use a business e-mail address for personal communications or whether the employee's position entails using an employer's device. Protective measures would include the lawyer refraining from sending e-mails

---

inapplicable to communications with counsel using workplace computer); Scott v. Beth Israel Medical Center, Inc., 847 N.Y.S.2d 436, 440-43 (N.Y. Sup. Ct. 2007) (privilege inapplicable to employer's communications with counsel via employer's e-mail system); Long v. Marubeni Am. Corp., No. 05CIV.639(GEL)(KNF), 2006 WL 2998671, at *3-4 (S.D.N.Y. Oct. 19, 2006) (e-mails created or stored in company computers were not privileged, notwithstanding use of private password-protected e-mail accounts); Kaufman v. SunGard Inv. Sys., No. 05-CV-1236 (JLL), 2006 WL 1307882, at *4 (D.N.J. May 10, 2006) (privilege inapplicable to communications with counsel using employer's network).

[5] For a discussion of a lawyer's duty when receiving a third party's e-mail communications with counsel, *see* ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 11-460 (2011) (Duty when Lawyer Receives Copies of a Third Party's E-mail Communications with Counsel).

[6] This opinion principally addresses e-mail communications, which are the most common way in which lawyers communicate electronically with clients, but it is equally applicable to other means of electronic communications.

to the client's workplace, as distinct from personal, e-mail address,[7] and cautioning the client against using a business e-mail account or using a personal e-mail account on a workplace computer or device at least for substantive e-mails with counsel.

As noted at the outset, the employment scenario is not the only one in which attorney-client electronic communications may be accessed by third parties. A lawyer sending or receiving substantive communications with a client via e-mail or other electronic means ordinarily must warn the client about the risk of sending or receiving electronic communications using a computer or other device, or e-mail account, to which a third party may gain access. The risk may vary. Whenever a lawyer communicates with a client by e-mail, the lawyer must first consider whether, given the client's situation, there is a significant risk that third parties will have access to the communications. If so, the lawyer must take reasonable care to protect the confidentiality of the communications by giving appropriately tailored advice to the client.

[7] Of course, if the lawyer becomes aware that a client is receiving personal e-mail on a workplace computer or other device owned or controlled by the employer, then a duty arises to caution the client not to do so, and if that caution is not heeded, to cease sending messages even to personal e-mail addresses.

AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 11-460 **August 4, 2011**

Duty when Lawyer Receives Copies of a Third Party's E-mail Communications with Counsel

When an employer's lawyer receives copies of an employee's private communications with counsel, which the employer located in the employee's business e-mail file or on the employee's workplace computer or other device, neither Rule 4.4(b) nor any other Rule requires the employer's lawyer to notify opposing counsel of the receipt of the communications. However, court decisions, civil procedure rules, or other law may impose such a notification duty, which a lawyer may then be subject to discipline for violating. If the law governing potential disclosure is unclear, Rule 1.6(b)(6) allows the employer's lawyer to disclose that the employer has retrieved the employee's attorney-client e-mail communications to the extent the lawyer reasonably believes it is necessary to do so to comply with the relevant law. If no law can reasonably be read as establishing a notification obligation, however, then the decision whether to give notice must be made by the employer-client, and the employer's lawyer must explain the implications of disclosure, and the available alternatives, as necessary to enable the employer to make an informed decision.

This opinion addresses a lawyer's ethical duty upon receiving copies of e-mails between a third party and the third party's lawyer.[1] We explore this question in the context of the following hypothetical scenario.

After an employee files a lawsuit against her employer, the employer copies the contents of her workplace computer for possible use in defending the lawsuit, and provides copies to its outside counsel. Upon review, the employer's counsel sees that some of the employee's e-mails bear the legend "Attorney-Client Confidential Communication." Must the employer's counsel notify the employee's lawyer that the employer has accessed this correspondence?[2]

When an employer's lawyer receives copies of an employee's private communications with counsel, which the employer located in the employee's business e-mail file or on the employee's workplace computer or other device, the question arises whether the employer's lawyer must notify opposing counsel pursuant to Rule 4.4(b). This Rule provides: "A lawyer who receives a document relating to the representation of the lawyer's client and knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender."

Rule 4.4(b) does not expressly address this situation, because e-mails between an employee and his or her counsel are not "inadvertently sent" by either of them. A "document [is] inadvertently sent" to someone when it is accidentally transmitted to an unintended recipient, as occurs when an e-mail or letter is misaddressed or when a document is accidentally attached to an e-mail or accidentally included among other documents produced in discovery. But a document is not "inadvertently sent" when it is retrieved by a third person from a public or private place where it is stored or left.

The question remains whether Rule 4.4(b) implicitly addresses this situation. In several cases, courts have found that Rule 4.4(b) or its underlying principle requires disclosure in analogous situations, such as when "confidential documents are sent intentionally and without permission." *Chamberlain Group, Inc. v. Lear Corp.*, 270 F.R.D. 392, 398 (N.D. Ill. 2010).[3] In *Stengart v. Loving Care Agency, Inc.*,

---

[1] This opinion is based on the ABA Model Rules of Professional Conduct as amended by the ABA House of Delegates through August 2011. The laws, court rules, regulations, rules of professional conduct, and opinions promulgated in individual jurisdictions are controlling.

[2] For a discussion of the employee's lawyer's obligation to take reasonable steps to prevent a situation such as this from arising, *see* ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 11-459 (2011) (Duty to Protect the Confidentiality of E-mail Communications With One's Client).

[3] *See also* Webb v. CBS Broadcasting, Inc., No. 08 C 6241, 2011 WL 1743338, at *12-13 (N.D. Ill. May 6, 2011); Burt Hill, Inc. v. Hassan, No. Civ.A. 09-1285, 2010 WL 419433, at *3-5 (W.D. Pa. Jan. 29, 2010); Allen v. Int'l Truck & Engine, No. 1:02-CV-0902-RLY-TAB, 2006 WL 2578896, at *11-12 (S.D. Ind. Sept. 6, 2006). *But see* Mt. Hawley Ins. Co. v. Felman Production, Inc., 271 F.R.D. 125, 130-31 (S.D. W. Va. 2010) (lawyer receiving inadvertently sent materials not required to notify another party or that party's

990 A.2d 650, 665 (N.J. 2010), the court found that the employer's lawyer in an employment litigation violated the state's version of Rule 4.4(b)[4] by failing to notify the employee's counsel that the employer had downloaded and intended to use copies of pre-suit e-mail messages exchanged between the employee and her lawyers.[5]

Since Rule 4.4(b) was added to the Model Rules, this Committee twice has declined to interpret it or other rules to require notice to opposing counsel other than in the situation that Rule 4.4(b) expressly addresses.[6] In ABA Formal Op. 06-442 (2006), we considered whether a lawyer could properly review and use information embedded in electronic documents (i.e., metadata) received from opposing counsel or an adverse party. We concluded, contrary to some other bar association ethics committees, that the Rule did not apply. We reasoned that "the recent addition of Rule 4.4(b) identifying the sole requirement of providing notice to the sender of the receipt of inadvertently sent information [was] evidence of the intention to set no other specific restrictions on the receiving lawyer's conduct."[7] Likewise, in ABA Formal Op. 06-440, this Committee found that Rule 4.4(b) does not obligate a lawyer to notify opposing counsel that the lawyer has received privileged or otherwise confidential materials of the adverse party from someone who was not authorized to provide the materials, if the materials were not provided as "the

---

lawyer of receipt as matter of compliance with ethics rules).

[4] The New Jersey rule provided: "[a] lawyer who receives a document and has reasonable cause to believe that the document was inadvertently sent shall not read the document or, if he or she has begun to do so, shall stop reading the document, promptly notify the sender, and return the document to the sender." New Jersey Rule of Professional Conduct 4.4(b) (2004).

[5] The *Stengart* court found that the employee "had an objectively reasonable expectation of privacy" in the e-mails based on the fact that the employee "could reasonably expect that e-mail communications with her lawyer through her personal account would remain private, and that sending and receiving them via a company laptop did not eliminate the attorney-client privilege that protected them." 990 A.2d at 655. In contrast, other decisions arising in different factual situations have found that the attorney-client privilege did not protect client-lawyer communications downloaded by an employer from a computer used by its employees. These other decisions have not suggested that the employer's lawyer had a notification duty when the employer provided copies of the employee's attorney-client communications to the employer's lawyer. *See, e.g.*, Long v. Marubeni Am. Corp., No. 05-CIV-639(GEL)(KNF), 2006 WL 2998671, at *4 (S.D.N.Y. Oct. 19, 2006); Kaufman v. SunGard Inv. Sys., No. 05-CV-1236 (JLL), 2006 WL 1307882, at *3 (D.N.J. May 9, 2006); Scott v. Beth Israel Medical Center, Inc., 847 N.Y.S.2d 436, 444 (Sup. Ct. 2007).

[6] One might argue, for example, that the lawyer is prohibited from reading or using the e-mails by any of several other rules. These include Rule 4.4(a), which requires lawyers to refrain from using "methods of obtaining evidence that violate [a third person's] legal rights," and which, according to the accompanying comment, forbids "unwarranted intrusions into privileged relationships, such as the client-lawyer relationship." These also include Rule 8.4(c), which forbids "conduct involving dishonesty, fraud, deceit or misrepresentation," and Rule 8.4(d), which forbids "conduct that is prejudicial to the administration of justice."

[7] ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-442 (2006) (Review and Use of Metadata). Prior to the adoption of Rule 4.4(b) in February 2002, this Committee had issued opinions addressing a lawyer's obligations upon receiving materials of an adverse party on an unauthorized basis when the lawyer knew that the materials were privileged or confidential, and addressing a lawyer's obligations when the opposing party inadvertently disclosed privileged or confidential materials. *See* ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 94-382 (1994) (Unsolicited Receipt of Privileged or Confidential Materials), in FORMAL AND INFORMAL ETHICS OPINIONS 1983-1998 (ABA 2000) at 233; ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 92-368 (1992) (Inadvertent Disclosure of Confidential Materials), *id*. at 140. The Committee concluded that the lawyer's obligations implicitly derived from other law and from provisions such as Rule 8.4 (prohibiting "conduct involving dishonesty, fraud, deceit or misrepresentation" and conduct "prejudicial to the administration of justice") that did not expressly address these situations. *Id*. at 144-49, 234. However, the Committee withdrew both of these opinions following the adoption of Rule 4.4(b). *See* ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-440 (2006) (Unsolicited Receipt of Privileged or Confidential Materials: Withdrawal of Formal Opinion 94-382); ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 05-437 (2005) (Inadvertent Disclosure of Confidential Materials: Withdrawal of Formal Opinion 92-368).

result of the sender's inadvertence."[8] We noted that other law might prevent the receiving lawyer from retaining and using the materials, and that the lawyer might be subject to sanction for doing so, but concluded that this was "a matter of law beyond the scope of Rule 4.4(b)."[9]

To say that Rule 4.4(b) and other rules are inapplicable is not to say that courts cannot or should not impose a disclosure obligation in this context pursuant to their supervisory or other authority. As Comment [2] to Rule 4.4(b) observes, "this Rule does not address the legal duties of a lawyer who receives a document that the lawyer knows or reasonably should know may have been wrongfully obtained by the sending person."[10] Pursuant to their supervisory authority, courts may require lawyers in litigation to notify the opposing counsel when their clients provide an opposing party's attorney-client confidential communications that were retrieved from a computer or other device owned or possessed by the client. Alternatively, the civil procedure rules governing discovery in the litigation may require the employer to notify the employee that it has gained possession of the employee's attorney-client communications. Insofar as courts recognize a legal duty in this situation, as the court in *Stengart* has done, a lawyer may be subject to discipline, not just litigation sanction, for knowingly violating it.[11] However, the Model Rules do not independently impose an ethical duty to notify opposing counsel of the receipt of private, potentially privileged e-mail communications between the opposing party and his or her counsel.

When the law governing potential disclosure is unclear, the lawyer need not risk violating a legal or ethical obligation. The fact that the employer-client has obtained copies of the employee's e-mails is "information relating to the representation of [the] client" that must be kept confidential under Rule 1.6(a) unless there is an applicable exception to the confidentiality obligation or the client gives "informed consent" to disclosure. Rule 1.6(b)(6) permits a lawyer to "reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary ... to comply with other law or a court order." Rule 1.6(b)(6) allows the employer's lawyer to disclose that the employer has retrieved the employee's attorney-client e-mail communications to the extent he or she reasonably believes it is necessary to do so to comply with the relevant law, even if the legal obligation is not free from doubt. On the other hand, if no law can reasonably be read as establishing a reporting obligation, then the decision whether to give notice must be made by the employer-client. Even when there is no clear notification obligation, it often will be in the employer-client's best interest to give notice and obtain a judicial ruling as to the admissibility of the employee's attorney-client communications before attempting to use them and, if possible, before the employer's lawyer reviews them. This course minimizes the risk of disqualification or other sanction if the court ultimately concludes that the opposing party's communications with counsel are privileged and inadmissible. The employer's lawyer must explain these and other implications of disclosure, and the available alternatives, as necessary to enable the employer to make an informed decision. *See* Rules 1.0(e) (Terminology, "informed consent"), 1.4(b) ("A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation"), and 1.6(a) ("lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by [the exceptions under Rule 1.6(b)]").

---

[8] *Supra* n. 7.

[9] *Id*. A recent article suggests that Rule 1.15(d) imposes a notification duty in the analogous situation in which a lawyer comes into possession of physical documents that appear to have been wrongly procured from another party. Brian S. Faughan & Douglas R. Richmond, "Model Rule 1.15: The Elegant Solution to the Problem of Purloined Documents," 26 ABA/BNA LAW. MAN. PROF. CONDUCT 623 (Oct. 13, 2010). Rule 1.15(d) provides, in pertinent part: "Upon receiving ... property in which a client or third person has an interest, a lawyer shall promptly notify the client or third person." The provision arises out of the lawyer's fiduciary duty to safeguard money and property belonging to another and entrusted to the lawyer. Regardless of whether this rule may apply when stolen physical items come into a lawyer's possession, we do not believe it applies when an organizational client gives its lawyer copies of documents that were on a computer in the client's lawful possession for the lawyer's potential use in litigation. What is at stake is not the third party's proprietary interest in the copies of e-mails but the third party's confidentiality interest, which Rule 1.15(d) does not address.

[10] *Accord* ABA Formal Op. 06-440.

[11] *See, e.g.*, Rule 3.4(c)("A lawyer shall not knowingly disobey an obligation under the rules of a tribunal except for an open refusal based on an assertion that no valid obligation exists.").

HOW TO MAKE YOUR FREE EMAIL POLICY

RocketLawyer.com

https://www.rocketlawyer.com/secure/interview/new.aspx?id=1425&utm_source=103&utm_medium=cpc&try=1&v=3&utm_account=RL-Docs-Search-Text-GDN&utm_campaign=Beta-Professional-Search&utm_adgroup=(1425)email-policy(professional)&utm_term=%252Bemail%2520%252Bpolicy&pkw=%252Bemail%2520%252Bpolicy&mkwid=s3UepwoXK_dc&pcrid=41793571505&pmt=b&plc=&gclid=CML_9OjHob0CFY1xOgod920ANQ#q1